

Digi TransPort User's Guide

90001019_K

14th April 2013

Contents

Introduction 11

Typographical Conventions 12

Warnings 13

Radio Equipment - Canadian Warning Statements 13

OEM Responsibilities 13

End Product Labeling 14

Radio Equipment - FCC Warning Statement 14

Obtaining Technical Support 16

Self help 16

Assisted help 16

Using the Web Interface 18

Access Via a LAN Port 18

Using the Command Line Interface 19

The “AT” Command Interface 19

Digi Application Commands 22

Establishing a Remote Connection 24

Configuring your TransPort router 25

Logging In 26

Configuring and Testing W-WAN Models 28

Signal Strength Indicators 29

Wizards 30

Configuration Page 31

Network Configuration 32

Interfaces 32

Ethernet 32

Wi-Fi 49

Mobile 58

DSL 72

GRE 79

ISDN 83

PSTN 99

DialServ 105

Serial 112

Advanced 126

DHCP Server 151
DHCP Server for Ethernet n 152
Logical Ethernet Interfaces 155
DHCP Options 155
Static Lease Reservations 156
Network Services 156
DNS Servers 158
DNS Server n 158
DNS Server Update 159
Dynamic DNS 162
Advanced 164
IP Routing / Forwarding - An introduction to TransPort routing 165
IP Routing 167
Static Routes 169
Route n 169
RIP 176
OSPF 180
BGP 181
IP Port Forwarding / Static NAT Mappings 183
Multicast Routes 184
Virtual Private Networking (VPN) 185
IPsec 185
L2TP 216
L2TP n 216
PPTP 219
OpenVPN 220
OpenVPN n 221
SSL 227
SSL Clients 227
SSL Server 228
SSH Server 229
SSH Server n 230
Configuring SSH 233
Configuration using the web interface 233
Configuration using the command line interface 234
SSH Authentication with a public/private keypair 234

FTP Relay 234
FTP Relay n 234
Advanced 237
IP Passthrough 237
UDP Echo 239
UDP Echo n 239
QoS 240
DSCP Mappings 241
Queue Profiles 242
Timebands 244
Timeband n 244
Advanced Network Settings 246
Legacy Protocols 250
SNA over IP 250
Legacy Protocols TPAD 257
Legacy Protocols TPAD n 257
X.25 267
Calls Macros 274
IP to X.25 Calls 274
MODBUS Gateway 290
Protocol Switch 293
CUD Mappings 303
IP Sockets to Protocol Switch 304
NUA to Interface Mappings 306
NUA Mappings 307
Alarms Configuration 309
Event Settings 309
Email Notifications 310
SNMP Traps 311
SMS Messages 312
Local Logging 313
Syslog Messages 313
Syslog Server n 314
Event Logcodes 315
Configuring Events 316
Configuring Reasons 318

SMTP Account 318
Systems Configuration 321
Device Identity 321
Date and Time 322
General 327
Remote Management Configuration 332
Device Cloud 332
Connection Settings 332
Advanced 333
SNMP 334
SNMP User > SNMP User n 336
SNMP Filters 337
SNMP Traps 337
Security Configuration 340
Users 340
User n 340
Firewall 342
Stateful Inspection Settings 344
RADIUS 345
RADIUS Client n 346
TACACS+ 350
Advanced 352
Command Filters 353
Calling Numbers 354
Position Configuration 356
GPS 356
Applications Page 360
Basic Applications 360
ScriptBasic 360
Python Applications 361
Python Files 361
Management Page 363
Network Status Management 364
Interfaces 364
Ethernet >ETH n 364
Wi-Fi 366

Mobile 369
DSL 373
GRE 375
ISDN 376
Serial > Serial n 378
Advanced > PPP > PPP n 380
IP Routing Table 383
IP Hash Table 384
Port Forwarding Table 386
Firewall 387
Firewall Trace 388
DHCP Status 390
DNS Status 390
QoS 391
Connections Management 392
IP Connections 392
Virtual Private Networking (VPN) Management 395
IPsec 395
IPsec Tunnels 395
IPsec peers 396
IKE SAs 397
Position Management 398
GPS 398
Event Log Management 400
Analyser Management 401
Settings 401
Trace 406
PCAP (e.g. Wireshark) traces 407
Top Talkers Management 408
Settings 408
Trace 409
Administration Page 410
System Information Administration 411
File Management Administration 413
FLASH Directory 413
WEB Directory 415

File Editor 416
X.509 Certificate Management Administration 417
Certificate Authorities (CAs) 417
IPsec/SSH/HTTPS Certificates 418
Key Generation 421
Update Firmware 423
Factory Default Settings 424
Execute a command 425
Save configuration 426
Reboot 427
Logout 428
Filing system & system files 429
Filing System Commands 430
USB Support 433
Universal config.da0 using tags 436
Web GUI Access via Serial Connection 439
SQL commands 449
Answering V.120 Calls 453
Initial Set Up 453
Initiating a V.120 Call 453
Answering V.120 Calls 453
ANSWERING ISDN CALLS 455
Protocol Entities 455
Multiple Subscriber Numbers 455
Multiple PPP Instances 456
X.25 PACKET SWITCHING 457
Introduction 457
B-channel X.25 457
D-channel X.25 457
X.28 Commands 458
PPP OVER ETHERNET 466
IPSEC AND VPNS 467
What is IPSec? 467
Data Encryption Methods 467
What is a VPN? 468
The Benefits of IPSec 468

X.509 Certificates 469
FIREWALL SCRIPTS 471
Introduction 471
Firewall Script Syntax 471
Specifying IP Addresses and Ranges 476
Address/Port Translation 478
Filtering on Port Numbers 478
Filtering on TCP Flags 479
Filtering on ICMP Codes 480
Stateful Inspection 481
The FWLOG.TXT File 486
Debugging a Firewall 490
REMOTE MANAGEMENT 491
Using V.120 491
Using Telnet 491
Using FTP 492
Using X.25 493
AT COMMANDS 494
D Dial 494
H Hang-up 494
Z Reset 494
&C DCD Control 495
&F Load Factory Settings 495
&R CTS Control 495
&V View Profiles 495
&W Write SREGS.DAT 495
&Y Set Default Profile 496
&Z Store Phone Number 496
\AT Ignore Invalid AT Commands 497
\LS Lock Speed 497
\PORT Set Active Port 497
\smib Commands 498
"S" REGISTERS 505
S0 V.120 Answer Enabled 505
S1 Ring count 506
S2 Escape Character 506

S12 Escape Delay 506
S15 Data Forwarding Timer 506
S23 Parity 506
S31 ASY Interface Speed 506
S33 DTR Dialling 507
S45 DTR Loss De-Bounce 507
GENERAL SYSTEM COMMANDS 508
CONFIG Show/Save Configuration 508
Config changes counter 508
REBOOT Reboot Unit 509
Reset router to factory defaults 509
Disabling the reset button 509
TEMPLOG Temperature monitoring 509
Ping and Traceroute 509
Clearing the Analyser Trace and Event Log 510
Activate and Deactivate interfaces 510
Special Usernames 510
GPIO (General Purpose Input Output) 510
GOBI Image Load Selection 512
TCPPERM AND TCPDIAL 513
TCPPERM 513
TCPDIAL 514
SERIAL PORT CONNECTIONS 515
DR6410, DR6420, DR6460, DR64x0W & WR41 516
WR44 519
TA2020 521
ER2110, IR2110 & MR2110 522
IR2140 & GR2140 523
GR2130 524
IR2140 527
IR2420 530
TA2020B & IR2110B 533
DR4410, DR4410i & DR4410p 536
MW3410, MW3520 & VC5100 539
ER4420, ER4420d, ER4420i, ER4420p, HR4420, HR4420d, HR4420i, HR4420p & IR4420 542

MR4110, ER4110, HR4110, GR4110 & TR4110 545
RS-232 (V.24) Serial Cable Wiring 548
Configuring X.21 on Older Models 551
EMAIL TEMPLATES 552
Template Structure 552
Certifications 555
GLOSSARY 557
ACKNOWLEDGEMENTS 563

Introduction

Thank you for choosing a data communications product from Digi International. Digi products are extremely versatile and may be used in a wide variety of applications. It would not be possible to describe in detail all such applications in a single guide. Consequently, this guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product, and of the requirements for their specific application.

Digi International designs and manufactures a wide range of both wireline and wireless network routing products. For a complete, up-to-date list of current products, please visit the Digi International web site at www.digi.com.

Whilst each of these models provide a different combination of hardware and software features, the basic method of configuration using the web interface or command line is the same in each case. This guide describes the operation of standard features available across the whole product range. Consequently, some of the features described in this guide may only be available on certain models or must be purchased as optional “feature packs”. You should refer to the specification of the particular model you have purchased to ascertain which features are supported as standard.

In addition to a comprehensive range of communications capabilities, our products provide a combination of powerful, yet easy to use, configuration, management and diagnostic tools. These include a protocol analyser, a time-stamped event log and remote management via the web interface or via a Telnet session.

In many applications, the serial ports will be configured to appear as if they were standard “AT” modems and behave accordingly. However, many other standard protocols are supported (e.g. B- and D-channel X.25, PPP, TPAD, V.120, etc.). This makes it simple and cost-effective to migrate existing terminal equipment, which uses the analogue telephone network, to faster, more reliable and cost effective “wireline” or wireless digital services.

All major features of the unit can be configured using a standard Web browser. This can be done locally (via a serial or LAN port), or remotely via a WAN connection. A built-in Web-server and flexible FLASH-memory based filing system mean that the unit can also be customised to provide application specific functions, statistics and diagnostic information.

Requests for corrections or amendments to this guide are welcome and should be addressed to:

Digi International
11001 Bren Road East
Minnetonka, MN 55343

Typographical Conventions

Throughout this manual certain typographical conventions are used as follows:

Text Type	Meaning
Text like this	... is standard text.
Note: Text like this ...	indicates points that are of particular importance.
Text like this ...	indicates commands entered by the user at the command line.
Text like this ...	indicates responses from the unit to commands you enter at the command line.
Configuration – Network > Interfaces	refers to the unit's web-based menu system.

Warnings

Radio Equipment - Canadian Warning Statements

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

This radio transmitter (identify the device by certification number, or model number if Category II) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Name / Model	Gain	Impedence
BEC C424-510065-A	1.8dBi	50Ω Nominal

OEM Responsibilities

The WR44v2 Module has been certified for integration into products only by OEM integrators under the following conditions:

1. The antenna(s) must be installed such that a minimum separation distance of 20cm is maintained between the radiator (antenna) and all persons at all times.
2. The transmitter module must not be co-located or operating in conjunction with any other antenna or transmitter.

As long as the two conditions above are met, further transmitter testing will not be required. However, the OEM integrator is still responsible for testing their end-product for any additional compliance requirements required with this module installed (for example, digital device emissions, PC peripheral requirements, etc.).

NOTE:
In the event that these conditions can not be met (for certain configurations or co-location with another transmitter), then Industry Canada certification is no longer considered valid and the IC Certification Number can not be used on the final product. In these circumstances, the OEM integrator will be responsible for re-evaluating the end product (including the transmitter) and obtaining a separate Industry Canada authorization.

End Product Labeling

The WR44v2 Module is labeled with its own IC Certification Number. If the IC Certification Number is not visible when the module is installed inside another device, then the outside of the device into which the module is installed must also display a label referring to the enclosed module. In that case, the final end product must be labeled in a visible area with either of the following:

- Contains Transmitter Module IC: 1846A-55M1644
- Contains IC: 1846A-55M1644

The OEM of the WR44v2 Module must only use the approved antenna(s) listed above, which have been certified with this module.

The OEM integrator has to be aware not to provide information to the end user regarding how to install or remove this RF module or change RF related parameters in the user's manual of the end product.

Important!

To comply with Industry Canada RF radiation exposure limits for general population, the antenna(s) used for this transmitter must be installed such that a minimum separation distance of 20cm is maintained between the radiator (antenna) and all persons at all times and must not be co-located or operating in conjunction with any other antenna or transmitter.

Radio Equipment - FCC Warning Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. End users must follow the specific operating instructions for satisfying RF exposure compliance. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

The antenna(s) used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons.

Any product using the WR44v2 Wi-Fi module must have a label stating 'Contains FCC ID: MCQ-55M1644B' placed on it in line with FCC labelling regulations.

Antenna Specification: RP-SMA

Attribute	Property
Frequency Range	2.4 to 2.5 GHz
Impedance	50 Ohm

Attribute	Property
VSWR	1.92 max
Return Loss	-10dB max
Gain	1.8 dBi
Polarization	Linear
Radiation Pattern	Near omni-directional in the horizontal plane
Admitted Power	1W
Electrical	1/2 λ Dipole

NOTE:
This module obtained its complete certificatipon by using the antenna described here. End users in North America should use an antenna that matches these specifications to maintain the module's certification. Antennas of the same type but operating with a lower gain may be used.

Obtaining Technical Support

Technical support for your Digi Transport router is readily available using the following methods.

Self help

Visit the Technical Support section of the Digi website at www.digi.com

From here, you can gain access to FAQs, knowledge base articles, application guides, quick setup guides, installation guides, software applications, firmware upgrades, product literature, warrantyregistration & a support forum.

Assisted help

To obtain support from the Digi Technical Support team, use one of the options below. The preferred method is either via the web portal or via email. This is because the support teams will ask for certain technical information which is required at the time the query is logged.

The support teams request that the following information is included with every support request:

- Hardware model
- Firmware revision
- Current configuration (config c show)
- Firewall configuration
- ADSL / Mobile status and relevant PPP status
- The event log

This information and more can be quickly and easily obtained from the router by downloading the single file debug.txt from ***Administration - Directory Listings > FLASH directory*** using the GUI, or, via the CLI with the command **`type debug.txt`** and send the output to a log file.

The file contents are created when the file is requested, so it may take a few seconds to create and download the file. **Please zip this file and include it with your support request.**

For more complex technical support queries, a detailed network diagram may also be requested.

Web portal

To log a support request online using the web portal, browse to www.digi.com and hover your mouse over the 'Support' link at the top of the page, select 'Online Support Request' from the dropdown list. The direct URL for the web portal is http://www.digi.com/support/eservice

You will need to create an account to use this service.

Remember to upload the debug.txt zip file!

Email

Email support is available from 2 locations:

UK

uksupport@digi.com

USA

support.wizards@digi.com

Remember to attach the debug.txt zip file to your email!

Telephone

Telephone support is available from 2 locations:

UK

Telephone support is available 09:00 - 17:30 GMT.

From within the UK: 0870 350 0035

International: +44 1943 605 055

USA

Telephone support is available 07:00 - 17:30 CST (GMT -6 Hours).

From within the Americas: 952 912 3456

International: +1 952 912 3456

Please be aware, we may ask you to submit your technical support query by email and include the debug.txt zip file.

Using the Web Interface

To access the built-in web pages using a web browser (e.g. Internet Explorer), there are two options.

To access the LAN port follow the instructions below. To access the web interface over a serial connection,see Web Access via Serial Connection.

Access Via a LAN Port

By default, the Digi Transport has a static IP address of 192.168.1.1 with DHCP server enabled. To acess the unit using a web browser (e.g. Internet Explorer), simply connect an Ethernet cable between the LAN port on the Digi Transport and your PC. Make sure your PC is setup to automatically receive an IP address by selecting **`Start > Control Panel > Network > Configuration`** and verifying the configuration.

Note:
All models are auto-sensing for 10/100 operation. Most models are also auto MDI/MDX, i.e. will automatically work with either a straight-through or cross-over cable. The only exceptions are the IR2140 and GR2130, which are NOT auto MDI/MDX

Using the Command Line Interface

Using a Web browser to modify text box or table values in the configuration pages is the simplest way to configure the unit and this process is described in the next chapter. However, if you do not have access to a Web browser, the unit can be configured using text commands. These commands may be entered directly at one of the serial ports or via a Telnet session. Remote configuration is also possible using Telnet or X.25.

To use the serial ports you will need a PC and some communications software such as HyperTerminal ™ (supplied with Windows) or TeraTerm™. The same commands may also be used to configure the unit remotely via Telnet, X.25 or V.120.

There are several types of text command:

AT Commands & S Registers

AT commands (pronounced “ay tee”) and Special registers (S registers) are supported in order to maintain compatibility with modems when the unit is used as a modem replacement.

Application Commands

Application commands are specific to Digi International products and are used to control most features of the unit when not using the Web interface.

X.3 Commands

These are standard X.3 commands which are used only in X.25 PAD mode

TPAD Commands

These are used only in TPAD mode.

The “AT” Command Interface

Command Prefix

The “AT” command prefix is used for those commands that are common to modems. To configure the unit using AT commands you must first connect it to a suitable asynchronous terminal.

You will first need to set the interface speed/data format for your terminal to 115,200bps, 8 data bits, no parity and 1 stop bit (these settings can be changed later if necessary). When your terminal is correctly configured, apply power and wait for the B2 indicator to stop flashing.

Unless you have previously configured the unit to automatically connect to a remote system on powerup, it will now be ready to respond to commands from an attached terminal and is in “command mode”.

Now type “AT” (in upper or lower case), and press [Enter]. The unit should respond with the message “OK”. This message is issued after successful completion of each command. If an invalid command is entered, the unit will respond with the message “ERROR”.

If there is no response, check that the serial cable is properly connected and that your terminal or PC communications software is correctly configured before trying again.

If you have local command echo enabled on your terminal, you may see the AT command displayed as “AATT”. If this happens you may use the “ATE0” command (which will appear as “AATTEE00”), to prevent the unit from providing command echo. After this command has been entered, further commands will be displayed without the echo.

The “AT” command prefix and the commands that follow it can be entered in upper or lower case. After the prefix, you may enter one or more commands on the same line of up to 40 characters. When the line is entered, the unit will execute each command in turn.

CLI parameter tables and how to use them

After every section, there will be a table that details the CLI parameters that relate to the web based parameters.

The CLI parameters nearly always take the following format, there are only a few exceptions.

<entity> <instance> <parameter> <value>

Where:

<entity> = eth, ppp, modemcc, wifi, ike, eroute, etc…

<instance> = 0, 1, 2, 3, etc… Some entities only use 0. Others have multiple instances.

<parameter> = The parameter name, such as, ipaddr, mask, gateway, etc...

<value> = The value to set, such as, off, on, 192.168.1.1, username, free_text, etc…

An example CLI parameter table would look like the following for Ethernet parameters.

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eth	n	descr	Free text field	Description
eth	n	ipaddr	Valid IP address	IP Address
eth	n	mask	Valid Subnet Mask	Mask
eth	n	gateway	IP address	Gateway
eth	n	dnsserver	IP address	DNS Server
eth	n	secdns	IP address	Secondary DNS Server
eth	n	dhcpcli	Off / On	On = Get an IP address automatically using DHCP Off = Use the following IP address

To use this table, read the row from left to right and replace the values as appropriate. Only the first 4 columns are needed for the CLI parameters, the right hand column shows the equivalent web based parameter.

If the **Instance** is **n** in the table, it is because there are multiple instances available. Use the instance number you need for your requirements.

If the **Instance** is set to a specific number, such as **0**, use the number specified in the table.

For example, to set a ‘Description’ of ‘Local LAN’ on Ethernet 0:

eth 0 descr “Local LAN”

Take note that because of the space between ‘Local’ and ‘LAN’, the wording is enclosed in double quotes.

To set an IP address on 192.168.1.1 on Ethernet 0:

eth 0 ipaddr 192.168.1.1

To set an IP address of 172.16.0.1 on Ethernet 1:

eth 1 ipaddr 172.16.0.1

To enable the DHCP client on Ethernet 2:

eth 2 dhcpcli on

The Escape Sequence

If you enter a command such as “ATD”, which results in the unit successfully establishing a connection to a remote system, it will issue a “CONNECT” result code and switch from command mode to on-line mode. This means that it will no longer accept commands from the terminal. Instead, data will be passed transparently through the unit to the remote system. In the same way, data from the remote system will pass straight through to your terminal.

The unit will automatically return to command mode if the connection to the remote system is terminated.

To return to command mode manually, you must enter a special sequence of characters called the “escape sequence”. This consists of three occurrences of the “escape character”, a pause (user configurable) and then “AT”. The default escape character is “+” so the default escape sequence is:

+++ *{pause}* AT

Entering this sequence when the unit is on-line will cause it to return to command mode but it will NOT disconnect from the remote system unless you specifically instruct it to do so (using “ATH” or another method of disconnecting). If you have not disconnected the call, the “ATO” command may be used to go back on-line.

Result Codes

Each time an AT command line is executed, the unit responds with a result code to indicate whether the command was successful. If all commands entered on the line are valid, the “OK” result code will be issued. If any command on the line is invalid, the “ERROR” result code will be issued.

Result codes may take the form of an English word or phrase (verbose code) or an equivalent number (numeric code), depending on the setting of the “ATV” command. Verbose codes are used by default.

The “ATV0” command can be used to select numeric codes if required. The results from the text based commands can be numeric or verbose. A full list of the Result codes is provided in the following table:

Numeric code	Verbose code	Meaning
0	OK	Command line executed correctly
1	CONNECT ISDN	connection established
2	RING	Incoming ring signal detected
3	NO CARRIER X.25	service not available
4	ERROR	Error in command line
6	NO DIALTONE ISDN	service not available
7	BUSY	B-channel(s) in use
8	NO ANSWER	No response from remote

“S” Registers

“S” (Special) registers are registers in the unit that are used to store certain types of configuration information. They are essentially a “legacy” feature included to provide compatibility with software that was originally designed to interact with modems. A full list of the registers is provided under the section heading “S registers”.

Digi Application Commands

The unit also supports numerous text-based “application” commands that are specific to Digi International products and do not require the “AT” prefix. Some of these are generic i.e. they are related to the general operation of the unit; others are application or protocol specific.

Application commands may be entered via any of the serial ports but if you are using ASY 0 or ASY 1 with auto-speed detection enabled (which is not possible on ports 2, 3, etc.), you must first lock the interface speed to the same as that of your terminal. To do this first ensure that the unit is responding to AT commands correctly and then enter the command:

AT\LS

The speed will remain locked until the unit goes on-line and then off-line again, the power is removed or the unit is reset. Once the port speed has been locked, “AT” commands will still work but you may also use the application commands.

Remember that if you subsequently re-enable auto-speed detection on the port it will disable the use of application commands until the “AT\LS” command has been re-entered or the port speed has been set to a specific speed using “S31”. For example, to set the port speed at 19,200bps enter the command:

ATS31=6

And then change your terminal settings to match.

Note:
Speed locking is not necessary when you use the text commands via a Telnet session.

Digi application commands (referred to just as text commands or CLI commands throughout the remainder of this guide), can be entered in upper or lower case but unlike “AT” commands, only one command may be entered on a line. After each successful command, the “OK” result code will be issued. An invalid command will cause the “ERROR” result code to be issued.

The general syntax for an application commands is:

<entity> <instance> <param_name> <value>

where:

<entity> is the name of the entity

<instance> is the instance number for the entity that you are configuring.

<param_name> is the name of the parameter that you wish to configure.

<value> is the new value for the specified parameter.

For example, to set the window size to 5 for X.25 PAD instance 1 you would enter:

pad 1 window 5

Even if there is only once instance of particular entity, you should only enter 0 for the instance number.

Wildcards in the CLI

Wildcards can be used in the field <param_name> when viewing parameters (not setting them), for example, to view all PPP 1 parameters that start with ‘r’ then command is:

ppp 1 r ?*

The output will show

```
ppp 1 r* ?
r_mru: 1500
r_acfc: OFF
r_pfc: OFF
r_pap: ON
r_chap: ON
r_accm: 0xffffffff
r_comp: OFF
r_addr: OFF
r_callb: 0
rxtimeout: 23
rdoosdly: 0
restdel: 2000
rebootfails: 0
rip: 0
ripip:
ripauth: 1
ripis: OFF
r_md5: 1
r_ms1: 1
r_ms2: 1
rbcast: OFF
OK
```

The Reboot Command

The **reboot** command is used to reboot the unit after altering the configuration. It has three modes of operation:

reboot - will reboot the unit after any FLASH write operations have been completed. Also, 1 second each is allowed for the following operations to be completed before reboot will take place:

• IPSec SA delete notifications have been created and sent

• TCP sockets have been closed

• PPP interfaces have been disconnected

reboot <n> - will reboot the unit in <n> minutes where n is 1 to 65,535

reboot cancel - will cancel a timed reboot if entered before the time period has passed.

The Active Port

When entering “AT” or text commands it is important to understand that in most cases, the command only affects the settings for the “active” port. This is usually the port to which you are physically connected but you may, if necessary, set the active port to another port of your choice using the “AT\PORT=N” command where “N” is 0-3.

Establishing a Remote Connection

• Once you have finished configuring the unit, there are several ways of establishing a link to a remote system:

• An outgoing V.120 call may be made using the “ATD” command

• You can initiate a DUN session to establish a dial-up PPP connection.

• An outgoing X.25 call may be made using the “ATD” command followed by the X.28 CALL command.

• An outgoing TPAD (Transaction PAD) call may be made by using the TPAD “a” (address) command followed by the appropriate NUA (this is normally only carried out under software control).

Similarly, incoming calls will be handled according to which protocols have been bound to the ASY ports and whether or not answering is enabled for each protocol.

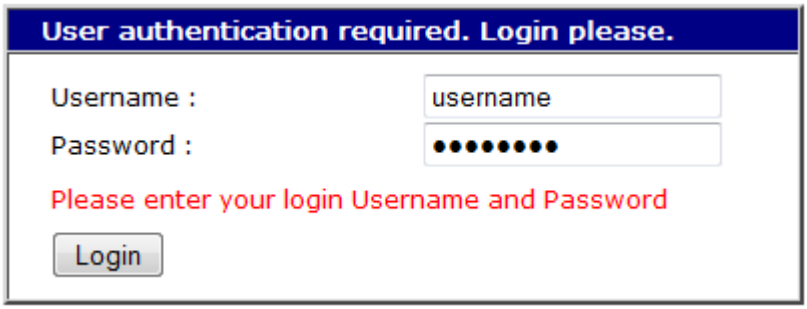
Configuring your TransPort router

This section describes the various configuration parameters for the unit and how to set or change them using the built-in web pages or the text commands. Configuration using the Web pages is achieved by entering the required values into text boxes or tables on the page, or by turning features on or off using checkboxes. The same results can be achieved entering the appropriate text commands via one of the serial ports.

Logging In

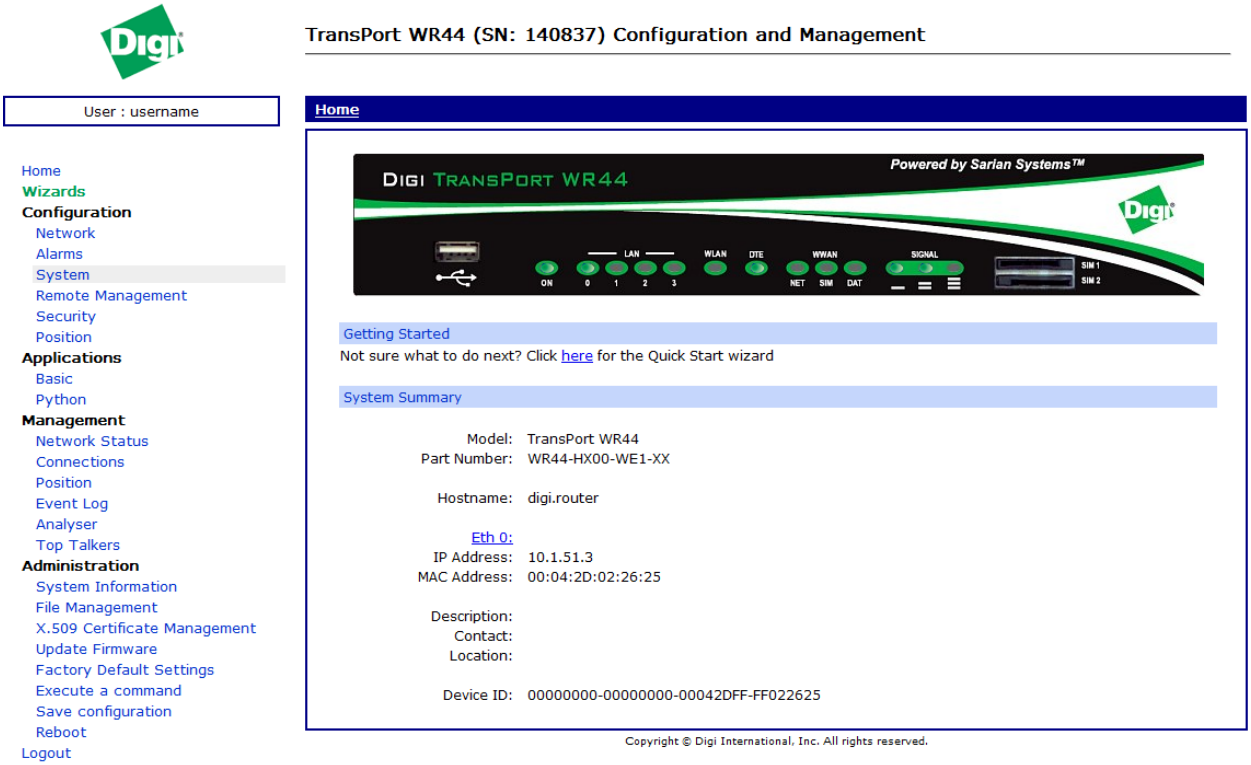
To configure the unit via the Web interface, either establish a DUN connection to it and then open your web browser and enter 1.2.3.4 for the web address, or enter the unit's Ethernet IP address (192.168.1.1) into your web browser after configuring your PC to have an address on the same subnet.

You will be presented with a login page similar to the following:



The default Username and Password are "username" and "password" respectively. Enter these and click the **Login** button to access the configuration pages. The password will be displayed as a series of dots for security purposes.

Correct entry of the username and password will display the main operations page similar to that shown below.

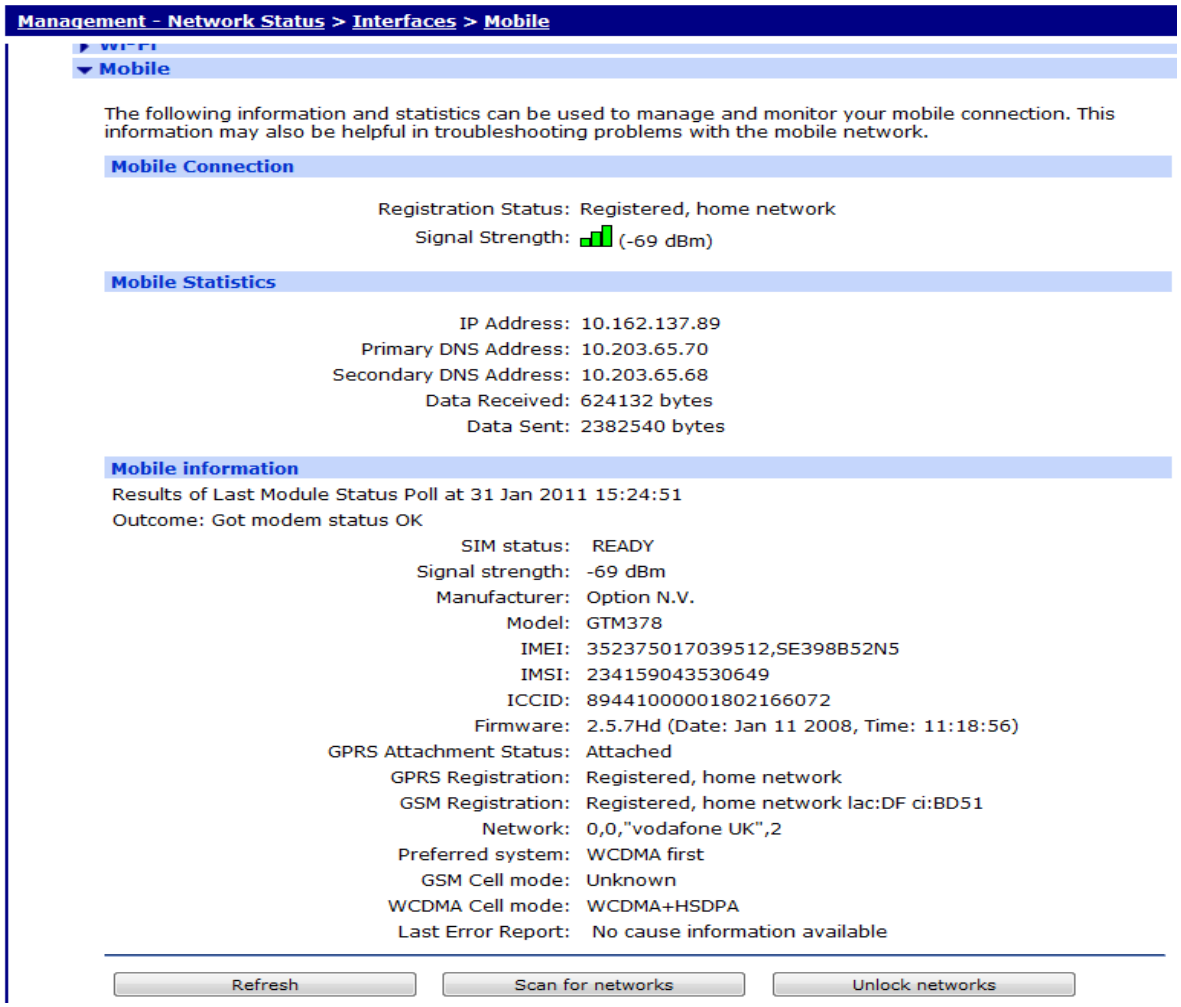


Clicking on the **Click to load Applet graphics!** button will display a representation of the front panel of your unit that will be updated every few seconds to show the actual status of the LED indicators. The model number of your unit will be shown at the top of the screen. The unit's serial number and ID are shown below the front panel representation.

Down the left side of the page you will see, the main menu with subsections which further expand when clicking on them.

Configuring and Testing W-WAN Models

Refer to the ***Configuration - Network > Interfaces > Mobile*** section of this guide to configure your router for the correct APN and PIN code (if any). You can now power up your unit and test connection to the wireless network. If you have correctly configured everything, the W-WAN SIM indicator on the front panel should illuminate green to show that a W-WAN enabled SIM card is present. The unit will now attempt to log on to the specified mobile network and if it is able to do so, the W-WAN NET indicator will illuminate steady. Data passing to and from the network will be reflected by the status of the DAT indicator, which will flash green. If you are unable to connect to the network, go to the ***Management - Network Status > Interfaces > Mobile*** web page and press the Refresh button. The page should appear similar to the following:


Management - Network Status > Interfaces > Mobile
Mobile
The following information and statistics can be used to manage and monitor your mobile connection. This information may also be helpful in troubleshooting problems with the mobile network.
Mobile Connection
Registration Status: Registered, home network
Signal Strength: (-69 dBm)
Mobile Statistics
IP Address: 10.162.137.89
Primary DNS Address: 10.203.65.70
Secondary DNS Address: 10.203.65.68
Data Received: 624132 bytes
Data Sent: 2382540 bytes
Mobile information
Results of Last Module Status Poll at 31 Jan 2011 15:24:51
Outcome: Got modem status OK
SIM status: READY
Signal strength: -69 dBm
Manufacturer: Option N.V.
Model: GTM378
IMEI: 352375017039512,SE398B52N5
IMSI: 234159043530649
ICCID: 89441000001802166072
Firmware: 2.5.7Hd (Date: Jan 11 2008, Time: 11:18:56)
GPRS Attachment Status: Attached
GPRS Registration: Registered, home network
GSM Registration: Registered, home network lac:DF ci:BD51
Network: 0,0,"vodafone UK",2
Preferred system: WCDMA first
GSM Cell mode: Unknown
WCDMA Cell mode: WCDMA+HSDPA
Last Error Report: No cause information available
Refresh
Scan for networks
Unlock networks

Note:
The signal strength is shown in “negative dB”, which means that the stronger the signal, the lower the number. As a guide -51dB would be a very strong signal, only normally obtained very close to a cell site. -115dB represents no signal. If your unit reports -115dB try reorienting the antenna or consider adding an external antenna.

Signal Strength Indicators

On units equipped with W-WAN modules, there are three LEDs on the front panel that will indicate the strength of the signal, as shown in the table below.

LEDs lit	Signal Strength
None	Under -113 dBm (effectively no signal)
1	-112 dBm to -87 dBm (weak signal)
2	-86 dBm to -71 dBm (medium strength signal)
3	-70 dBm to -51 dBm (strong signal)

The minimum recommended strength indication is 2 LEDs. If you have no or 1 LEDs lit, it is recommended that you fit an external antenna to the unit.

Wizards

This page contains wizards that simplify common configuration tasks. These wizards will change the minimum number of parameters to complete the required configuration task. However, due to the generic nature of the wizards they may not be suitable for all circumstances.

Quick Start Wizard

The Quick Start Wizard will display the options required for basic configuration of the Eth 0, WLAN and WWAN interfaces.

LAN to LAN IPsec Tunnel Wizard

This wizard will help you to configure an aggressive mode LAN to LAN IPsec tunnel to a remote host.

GOBI Module Carrier Wizard

Used with routers that have a GOBI module installed, to configure the router for a specified WWAN carrier.

Dual SIM Wizard

Use this wizard to configure the router to detect a link failure and automatically switch to the second installed SIM. This wizard only helps to configure the most commonly used methods of link error detection. There are more options detailed in Application Note 7 which can be found on the TransPort Support pages of the Digi website.

Note:

The wizards are designed to assist users. For very specific or uncommon requirements then further manual configuration may be required after completing any of the above wizards.

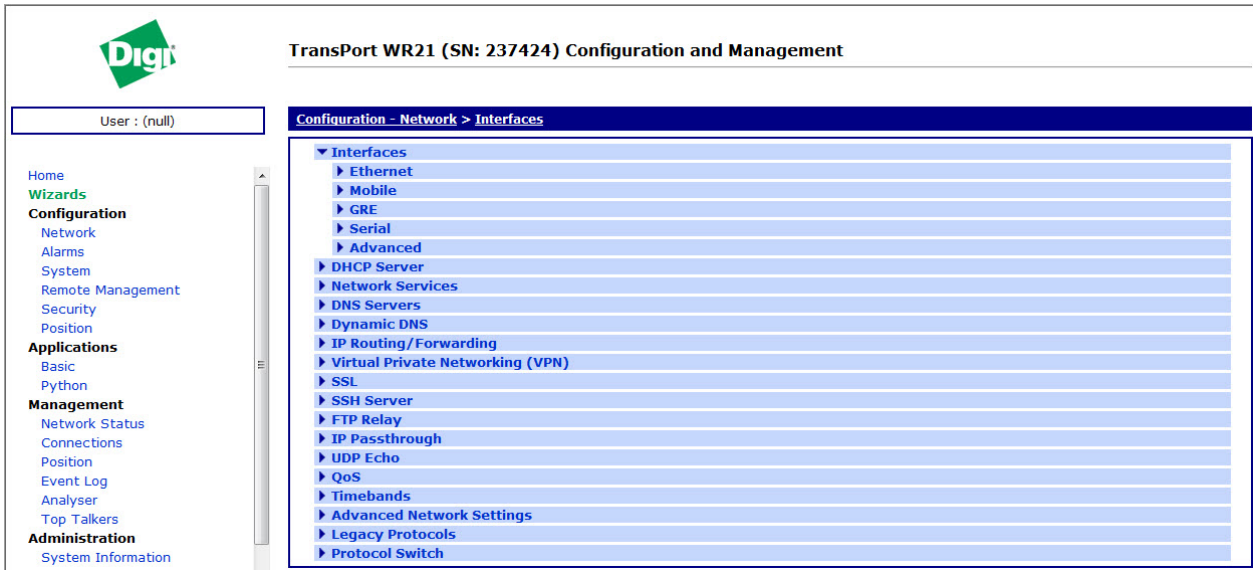
Configuration Page

Configuration page offers the following options:

- Network Configuration
- Alarms Configuration
- Systems Configuration
- Remote Management Configuration
- Security Configuration
- Positions Configuration

Network Configuration

The ***Configuration - Network*** page has the following options:



Interfaces

Configuration – Network> Interfaces

The ***Configuration – Network> Interfaces*** menu offers the following options:

- Ethernet
- Mobile
- GRE
- Serial
- Advanced

Ethernet

Configuration – Network> Interfaces> Ethernet

Underneath the Ethernet sub menus, there are configuration parameters for:

- Physical Ethernet interfaces (ETHn)
- Logical Ethernet Interfaces
- MAC Filtering
- MAC Bridging
- Spanning Tree Protocols(RSTP)
- VLANs

The ***Configuration - Network > Interfaces > Ethernet*** folder opens to list configuration pages for each of the available Ethernet instances on the unit. Each page allows the user to configure parameters such as the IP address, mask, gateway, etc.

On units with only one Ethernet port, if more than one Ethernet instance exist these are treated as logical Ethernet ports. These instances can be used to assign more than one Ethernet IP address to a router.

On units with more than one physical Ethernet port, the Ethernet instances refer to the different physical Ethernet ports. These units can be configured for either “HUB” mode or “Port Isolate” mode.

In HUB mode all the Ethernet ports are linked together and behave like an Ethernet hub or switch. This means that the router will respond to all of its Ethernet IP addresses on all of its ports (as the hub/ switch behavior links the ports together).

In Port Isolate mode the router will only respond to its Ethernet 0 IP address on physical port “LAN 0”, its Ethernet 1 IP address on physical port “LAN 1”, etc. The router will not respond to its Ethernet 1 address on port “LAN 0” unless routing has been configured appropriately.

When configured for HUB mode it is important that no more than one of the router’s ports is connected to another hub or switch on the same physical network otherwise an Ethernet loop can occur. The default behavior is “HUB” rather than “Port Isolate”.

Note:
VLAN tagging is not available when the router is configured for Port Isolate mode.

ETHn

This initial view only shows basic IP address parameters. The choice is to obtain an IP address by using a DHCP server or to manually configure the IP addressing for this interface.

Description
This parameter allows you to enter a name for this Ethernet instance, to make it easier to identify.

Get an IP address automatically using DHCP
Selecting this option enables the DHCP client on this interface.

Use the following IP address
Selecting this option enables manual configuration of the IP addressing parameters

IP Address
This parameter specifies the IP address of this Ethernet port on your LAN.

Mask
This parameter specifies the subnet mask of the IP subnet to which the unit is attached via this Ethernet port. Typically, this would be 255.255.255.0 for a Class C network.

Gateway
This parameter specifies the IP address of a gateway to be used by the unit. IP packets whose destination IP addresses are not on the LAN to which the unit is connected will be forwarded to this gateway.

DNS Server / Secondary DNS Server
These parameters specify the IP address of DNS servers to be used by the unit for resolving IP hostnames.

Note:

If the IP address, Mask, Gateway, DNS server or Secondary DNS server parameters are specified manually, but the option to use a DHCP server is later selected, any existing manually specified parameters will override the DHCP supplied parameters. To change from manual configuration to DHCP, be sure to remove all manually specified parameters first.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eth	n	descr	Free text field	Description
eth	n	ipaddr	Valid IP address	IP Address
eth	n	mask	Valid Subnet Mask	Mask
eth	n	gateway	IP address	Gateway
eth	n	dnsserver	IP address	DNS Server
eth	n	secdns	IP address	Secondary DNS Server
eth	n	dhcpcli	on, off	On = Get an IP address automatically using DHCP Off = Use the following IP address

Advanced

Configuration – Network> Interfaces> Ethernet> Eth n> Advanced

On units with only one Ethernet port, there may be multiple configurable Ethernet instances. Ethernet 0 is the physical interface. These extra instances are treated as logical Ethernet ports and can be used to assign more than one Ethernet IP address to a router.

On units with more than one physical Ethernet port, the Ethernet instances refer to the different physical Ethernet ports. These units can be configured for either “HUB” mode or “Port Isolate” mode.

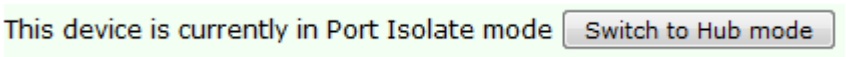
In HUB mode all the Ethernet ports are linked together and behave like an Ethernet hub or switch. This means that the router will respond to all of its Ethernet IP addresses on all of its ports (as the hub/ switch behaviour links the ports together).

In Port Isolate mode the router will only respond to its Ethernet 0 IP address on physical port “LAN 0”, its Ethernet 1 IP address on physical port “LAN 1”, etc. The router will not respond to its Ethernet 1 address on port “LAN 0” unless routing has been configured appropriately.

When configured for HUB mode it is important that no more than one of the router’s Ethernet interfaces is connected to another hub or switch on the same physical network otherwise an Ethernet loop can occur. The default behaviour is “HUB” rather than “Port Isolate”.

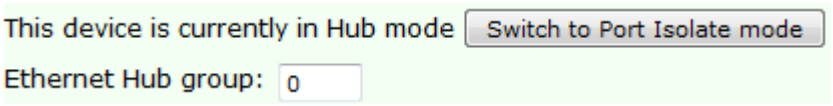
Port Isolate mode

If the router is running in Port Isolate mode, the following will be displayed, with an option to switch to Hub mode.



Hub Mode (factory default)

If the router is running in Hub mode, the following will be displayed, with an option to switch to Port Isolate mode.



Ethernet Hub group

On units with a built-in hub/switch, the Ethernet Hub Group parameter for each port is normally set to 0. This means that all ports "belong" to the same hub. If required however, the Hub Group parameter may be used to isolate specific ports to create separate hubs. For example, if Ethernet 0 and Ethernet1 have their Group parameter set to 0 whilst Ethernet 2 and Ethernet 3 have their Group parameter set to 1, the unit will in effect be configured as two 2-port hubs instead of one 4-port hub. This means that traffic on physical ports "LAN 0" and "LAN 1" will not be visible to traffic on physical ports "LAN 2" and "LAN 3" (and vice versa). Group numbers can be 0 – 3 or use 255 for an interface to be in all groups.
This parameter is not available on the web page when the unit is configured for Port Isolate mode.

Metric
This parameter specifies the connected metric of an interface, changing this value will alter the metric of dynamic routes created automatically for this interface. The default metric of a connected interface is 1. By allowing the interface to have a higher value (lower priority), static routes can take preference to interface generated dynamic routes. For normal operation, leave this value unchanged.

MTU
This parameter is used to set the Maximum Transmit Unit for the specified interface. The default value is 0 meaning that the MTU will either be 1504 (for units using a Kendin Ethernet device) or 1500 (for non-Kendin devices). The non-zero, values must be greater than 128 and not more than the default value. Values must also be multiples of 4 and the unit will automatically adjust invalid values entered by the user. So, if the MTU is set to 1000, the largest IP packet that the unit will send is 1000 bytes.

Enable auto-negotiation
Selecting this option allows the router and the other Ethernet device it is connected to, to auto-negotiate the speed and duplex of the Ethernet connection.

Speed (currently 100Base-T)
This parameter is used to select "10Base-T", "100Base-T" or "Auto" mode. The currently selected mode will be shown in brackets after the parameter name.
Note, enabling 'Auto-negotiation' AND manually setting the speed will only allow the selected speed to be negotiated.

Duplex
This parameter is used to select "Full Duplex", "Half Duplex" or "Auto" mode.
Note, enabling 'Auto-negotiation' AND manually setting the Duplex will only allow the selected Duplex mode to be negotiated.

Max Rx rate
On models with multiple Ethernet interfaces, this parameter may be used to specify a maximum data rate in kbps that the unit will receive on this interface. This may be useful in applications where separate Ethernet interfaces are allocated to separate LANs and it is necessary to prioritize traffic from one LAN over another.

Max Tx rate

On models with multiple Ethernet interfaces, this parameter may be used to specify a maximum data rate in kbps that the unit will transmit on this interface. This may be useful in applications where separate Ethernet interfaces are allocated to separate LANs and it is necessary to prioritize traffic from one LAN over another.

TCP transmit buffer size
When set to a non-zero value, this parameter sets the TCP buffer size of transmitted packets in bytes. This is useful for slow / lossy connections such as satellite. Setting this buffer to a low value will prevent the amount of unacknowledged data from getting too high. If retransmits are required, a smaller TX buffer helps prevent retransmits flooding the connection.

Take this interface out of service after n seconds when the link is lost (e.g. cable removed or broken)
This parameter is used to specify the length of time (in seconds) that the router will wait after detecting that an Ethernet cable has been removed before routes that were using that interface are marked as out of service. If the parameter is set to 0, the feature is disabled i.e. routes using the interface will not be marked as out of service if the cable is removed.

Enable NAT on this interface
This parameter is used to select whether IP Network Address Translation (NAT) or Network Address and Port Translation (NAPT) are used at the Ethernet interface. When the parameter is set to disabled, no NAT will take place. When this parameter is enabled, extra options described below will be displayed.

NAT and NAPT can have many uses but they are generally used to allow a number of private IP hosts (PCs for example) to connect to the Internet through a single shared public IP address. This has two main advantages, it saves on IP address space (the ISP only need assign you one IP address), and it isolates the private IP hosts from the Internet (effectively providing a simple firewall because unsolicited traffic from the Internet cannot be routed directly to the private IP hosts.

To use NAT or NAPT correctly in the example of connecting private hosts to the Internet, NAT or NAPT should be enabled on the router's WAN side interface and should be disabled on the router's LAN side interface.

IP address
When a private IP host sends a UDP or TCP packet to an Internet IP address, the router will change the source address of the packet from the private host IP to the router's public IP address before forwarding the packet onto the Internet host. Additionally it will create an entry in a "NAT table" containing the private IP source address, the private IP port number, the public IP destination address and the destination port number. Conversely, when the router receives a reply packet back from the public host, it checks the source IP, source port number and destination port number in the NAT table to determine which private host to forward the packet to. Before it forwards the packet back to the private host, it changes the destination IP address of the packet from its public IP address to the IP address of the private host.

IP address and Port
This mode behaves like NAT but in addition to changing the source IP of the packet from the private host it can also change the source port number. This is required if more than one private host attempts to connect using the same local port number to the same Internet host on the same remote port number. If such a scenario were to occur with NAT the router would be unable to determine which private host to route the returning packets to and the connection would fail.

Enable IPsec on this interface
This parameter is used to enable or disable IPSec security features for this Ethernet interface.

Use interface x,y for the source IP address of IPsec packets
By default, the source IP address for an IPsec Eroute will be the IP address of the interface on which IPSec was enabled. By setting this parameter to either PPP or Ethernet and the relevant interface number, the source address used by IPSec will match that of the Ethernet or PPP interface specified.

Enable the firewall on this interface
This parameter is used to turn Firewall script processing "On" or "Off" for this interface.

Remote management access
The Remote access options parameter can be set to "No restrictions", "Disable management", "Disable return RST", "Disable management & return RST". When set to "No restrictions", users on this interface can access the unit's Telnet, FTP and web services for the purpose of managing the unit.

When set to "Disable management", users on this interface are prevented from managing the unit via Telnet, FTP or the web interface.

Disable return RST - whenever a unit receives a TCP SYN packet for one of its own IP addresses with the destination port set to an unexpected value, i.e. a port that the unit would normally expect to receive TCP traffic on, it will reply with a TCP RST packet. This is normal behaviour.

However, the nature of internet traffic is such that whenever an internet connection is established, TCYP SYN packets are to be expected. As the router's PPP inactivity timer is restarted each time the unit transmits data (but not when it receives data), the standard response of the unit to SYN packets i.e. transmitting an RST packet, will restart the inactivity timer and prevent the unit from disconnecting the link even when there is no "genuine" traffic. This effect can be prevented by using the appropriate commands and options within the firewall script. However, on Digi 1000 series units, or where you are not using a firewall, the same result can be achieved by selecting this option, i.e. when this option is selected the normal behaviour of the unit in responding to SYN packets with RST packets is disabled. The option will also prevent the unit from responding to unsolicited UDP packets with the normal ICMP destination unreachable responses.

The "Disable management & return RST" option prevents users from managing the unit via the Telnet, FTP and web interfaces and also disables the transmission of TCP RST packets as above.

Multihome additional consecutive addresses
This parameter defines how many additional (consecutive) addresses the ethernet driver will "own". For example, if the IP address of the interface was 10.3.20.40, and Multihome additional consecutive addresses was set to 3, the IP addresses 10.3.20.41, 10.3.20.42 and 10.3.20.43 would also belong to the Ethernet interface.

Respond to ARP requests only if the requestor is of this network

When this parameter is enabled, the ethernet context will only respond to ARP requests if the source IP in the ARP request is of the network configured into the ethernet instance.

Enable IGMP on this interface

This parameter is used to enable or disable the Internet Group Management Protocol for this Ethernet interface.

Enable Bridge on this interface
Bridge mode only applies to models with built in Wi-Fi. If Wi-Fi is enabled, bridge mode must be enabled on the Eth 0. This will create an Ethernet bridge between the Wi-Fi access point and the physical Ethernet interface.

Generate Heartbeats on this interface
Enabling this option will display the parameters for Heartbeat packets. These are UDP packets which can contain status information about the router and can be used in conjunction with Remote Manager.

Send Heartbeat messages to IP address a.b.c.d every h hrs m mins s seconds
Where:
a.b.c.d specifies the destination IP address for heartbeat packets.
h, m & s specifies how often the router will transmit "heartbeat" packets to the specified destination in (h) Hours, (m) Minutes and (s) Seconds.

Use interface x,y for the source IP address
By default, heartbeat packets will be sent with the source IP address of the interface on which they were generated. If the heartbeat is required to be sent via an IPSec tunnel, this parameter can be used to specify the source IP address of the heartbeat packet to ensure the source and destination match the eroute selectors.

Select the transmit interface using the routing table
When enabled, the UDP heartbeats will choose the best route from the routing table. If disabled the exit interface will be interface on which the heartbeat is configured.

Include IMSI information in the Heartbeat message
When enabled, the heartbeat will include the IMSI of the cellular module.

Include GPS information in the Heartbeat message
When enabled and the appropriate GPS hardware is installed, the heartbeat will include the GPS co-ordinates of the router.

Generate Ping packets on this interface
Enabling this option will display the parameters for enabling auto-pings to be transmitted from this interface. These pings can be monitored by the interface auto-pings were enabled on and in the event of no ping reply, the interface can be taken out of service for a specified amount of time, before allowing the interface to be used again. Another option is to enable auto-pings on this interface and let the firewall handle taking the interface out of service in the event of a failure. Both methods are explained in Application Notes on our Technical Support Documents webpage.

Send n byte pings to IP host a.b.c.d every h hrs m mins s seconds
Where:
n specifies the payload size of a ping packet when used with the auto ping feature. Leaving this parameter blank will use the default value.
a.b.c.d specifies the destination IP address for auto-ping ICMP echo request.
h, m & s specifies how often the router will transmit "Auto-ping" packets to the specified destination in (h) Hours, (m) Minutes and (s) Seconds.

Switch to sending pings to IP host a.b.c.d after n failures
Where:
a.b.c.d specifies an alternative destination IP address for the auto-ping ICMP echo request to be sent to, should the main IP address specified in the parameter above fail to respond. This allows the router to double check there is a problem with the connection

and not just with the remote device not responding.
n specifies the number pings that need to fail before the 2nd IP address is checked. The extra IP address check is only enabled if this parameter is set to something other than 0.

Only send Pings when this Ethernet interface is "In Service"
If this parameter is enabled, ICMP echo requests will only be sent from this interface when it is in service. The default setting is disabled, ICMP echo requests are sent when the interface is in service and out of service.

Take this interface "Out of Service" after receiving no responses for s seconds
This parameter is used to specify the length of time in (s) seconds, before a route will be designated as being out of service if there has been no response to ANY of the ICMP echo requests during that time period.

Keep this interface out of service for s seconds
This parameter is used to specify the length of time in (s) seconds, for which any routes using this Ethernet interface will be held out of service after a ping failure is detected.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
n/a	n/a	ethvlan	n/a	Switch to Port Isolate Mode
n/a	n/a	ethhub	n/a	Switch to Hub Mode
eth	n	group	0 - 3,255	Ethernet Hub group
eth	n	metric	1 - 16	Metric
eth	n	mtu	64 - 1500	MTU
eth	n	auton	0,1	Enable auto-negotiation
eth	n	speed	0,10,100	Speed 0 = Auto 10 = 10-BaseT 100 = 100-BaseT
eth	n	duplex	0,1,2	Duplex 0 = Auto 1 = Full 2 = Half
eth	n	maxkbps	value in kbps	Max Rx rate
eth	n	maxtkbps	value in kbps	Max Tx rate
eth	n	tcptxbuf	value in bytes	TCP transmit buffer size
eth	n	linkdeact	0 - 86400	Take this interface out of service after n seconds when the link is lost
eth	n	do_nat	0,1,2	Enable NAT on this interface 0 = Disabled 1 = IP address 2 = IP address and Port
eth	n	ipsec	0,1	Enable IPsec on this interface
eth	n	ipsecent	blank,ETH,PPP	Use interface x,y for the source IP

Entity	Instance	Parameter	Values	Equivalent Web Parameter
				address of IPsec packets x = Interface type
eth	n	ipsecadd	0 - 255	Use interface x,y for the source IP address of IPsec packets y = interface number
eth	n	firewall	0,1	Enable the firewall on this interface
eth	n	nocfg	0,1,2,3	Remote management access 0 = No restrictions 1 = Disable management 2 = Disable return RST 3 = Disable management and return RST
eth	n	mhome	0 - 255	Multihome additional consecutive addresses
eth	n	arpnetonly	0, 1 (default: OFF)	Respond to ARP requests only if the requestor is of this network
eth	n	igmp	0,1	Enable IGMP on this interface
eth	n	bridge	0,1	Enable Bridge on this interface
eth	n	heartbeatip	IP address	Send Heartbeat messages to IP address a.b.c.d every h hrs m mins s seconds
eth	n	hrtbeatint	0 - 86400	Send Heartbeat messages to IP address a.b.c.d every h hrs m mins s seconds This CLI value is entered in seconds only.
eth	n	hbipent	blank,ETH,PPP	Use interface x,y for the source IP address x = Interface type
eth	n	hbipadd	0 - 255	Use interface x,y for the source IP address y = interface number
eth	n	hbroute	0,1	Select the transmit interface using the routing table
eth	n	hbimsi	0,1	Include IMSI information in the Heartbeat message
eth	n	hbgps	0,1	Include GPS information in the Heartbeat message
eth	n	pingsiz	value in bytes	Send n byte pings to IP host a.b.c.d every h hrs m mins s seconds
eth	n	pingip	IP address	Send n byte pings to IP host a.b.c.d every h hrs m mins s seconds

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eth	n	pingint	0 - 86400	Send n byte pings to IP host a.b.c.d every h hrs m mins s seconds This CLI value is entered in seconds only.
eth	n	pingint2	0 - 86400	No PING response request interval (s).
eth	n	pingip2	IP address	Switch to sending pings to IP host a.b.c.d after n failures
eth	n	ip2count	0 - 255	Switch to sending pings to IP host a.b.c.d after n failures
eth	n	pingis	0,1	Only send Pings when this Ethernet interface is "In Service"
eth	n	pingoos	0 - 86400	Take this interface "Out of Service" after receiving no responses for s seconds
eth	n	oossecs	0 - 86400	Keep this interface out of service for s seconds

QoS

Configuration – Network> Interfaces > Ethernet > Eth n> QoS

The parameters on this page control the Quality of Service management facility. Each Ethernet interface has an associated QoS instance, where ETH 0 maps to QoS 5, ETH 1 maps to QoS 6 and so on. These QoS instances include ten QoS queues into which packets may be placed when using QoS. Each of these queues must be assigned a queue profile from the twelve available.

Enable QoS on this interface
This checkbox, when checked, reveals the following QoS configuration parameters:-

Link speed n Kbps
The value in this text entry box should be set to the maximum data rate that this PPP link is capable of sustaining. This is used when calculating whether or not the data rate from a queue may exceed its minimum Kbps setting as determined by the profile assigned to it and send at a higher rate (up to the maximum Kbps setting).

Queue n
Below this column heading, is a list of ten queue instances. Each instance is associated with the profile and priority on the same row.

Profile n
This column contains the profile to be associated with the queue. There are twelve available, 0 – 11, which are selected from the drop-down list boxes.

Priority
This column contains drop-down menu boxes which are used to assign a priority to the selected queue. The priorities available are: “Very High”, “High”, “Medium”, “Low”, and “Very Low”.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
qos	n	linkkbps	Integer	Link speed n kbps
qos	n	q0prof	0 - 11	Queue 0 Profile
qos	n	q0prio	0 – 4 0 = Very high 1 = High 2 = Medium 3 = Low 4 = Very Low	Queue 0 Priority
qos	n	q1prof	0 – 11	Queue 1 Profile
qos	n	q1prio	0 – 4	Queue 1 Priority
qos	n	q2prof	0 - 11	Queue 2 Profile
qos	n	q2prio	0 – 4	Queue 2 Priority
qos	n	q3prof	0 - 11	Queue 3 Profile
qos	n	q3prio	0 – 4	Queue 3 Priority
qos	n	q4prof	0 - 11	Queue 4 Profile
qos	n	q4prio	0 – 4	Queue 4 Priority
qos	n	q5prof	0 - 11	Queue 5 Profile
qos	n	q5prio	0 – 4	Queue 5 Priority
qos	n	q6prof	0 - 11	Queue 6 Profile
qos	n	q6prio	0 – 4	Queue 6 Priority
qos	n	q7prof	0 - 11	Queue 7 Profile
qos	n	q7prio	0 – 4	Queue 7 Priority
qos	n	q8prof	0 - 11	Queue 8 Profile
qos	n	q8prio	0 – 4	Queue 8 Priority
qos	n	q9prof	0 - 11	Queue 9 Profile
qos	n	q9prio	0 – 4	Queue 9 Priority

VRRP

Configuration – Network> Interfaces > Ethernet> Eth n> VRRP

VRRP (Virtual Router Redundancy Protocol) allows multiple physical routers to appear as a single gateway for IP communications in order to provide back-up WAN communications in the event that the primary router in the group fails in some way. It works by allowing multiple routers to monitor data on the same IP address. One router is designated as the "Master" of the address and under normal circumstances it will route data as usual. However, the VRRP protocol allows the other routers in the VRRP group to monitor the "Master" and if, they detect that it is no longer operating, negotiate with each other to take over the role as owner. The protocol also facilitates the automatic re-prioritization of the original owner when it returns to operation.

Enable VRRP on this interface
This parameter enables VRRP on this interface.

VRRP Group ID
The VRRP group ID parameter is used to identify routers that are configured to operate within the same VRRP group. The default value is 0 which means that VRRP is disabled on this Ethernet interface. The value may be set to a number from 1 to 255 to enable VRRP and include this Ethernet port in the specified VRRP group.

VRRP Priority
This parameter is used to set the priority level of this Ethernet interface within the VRRP group from 0 to 255. 255 is the highest priority and setting the priority to this value would designate this Ethernet interface as the initial "Master" within the group. The value selected for the VRRP priority should reflect the values selected for other routers within the VRRP group, i.e. no two routers in the group should be initialized with the same value.

Boost the priority by n for s seconds after switching to the MASTER state
Increases the VRRP priority by the specified amount for the specified amount of time when the router has become the VRRP group master. The reason for why you might want to do this is to provide some network stability if the original Master keeps going on and off line thus causing a lot of VRRP state switches.

Enable VRRP+ Probing
This parameter enables VRRP+ probing on this Ethernet interface.

VRRP with probing differs from standard VRRP in that it dynamically adjusts the VRRP priority of an interface and if necessary, changes the status of that interface from "master" to "backup" or vice-versa. It does this by "probing" an interface, either by sending an ICMP echo request (PING) or by attempting to open a TCP socket to the specified Probe IP address. Hence VRRP operation is enhanced to ensure that a secondary router can take over under a wider range of circumstances.

Send p probe to IP address a.b.c.d TCP port n
Configures VRRP+ to send a probe packet to desired IP address and TCP port. The TCP port is needed if the probe type is TCP.
The routing code is used to determine which interface should be used. This allows the unit to test other interfaces and adjust the VRRP priority according to the status of that interface. For example, the user may wish to configure probing in such a way that the Digi router WAN interface is tested, and adjust the VRRP priority down if the WAN is not operational. Another example would be to probe the WAN interface of another VRRP router, and adjust the local VRRP priority up if that WAN interface isn't operational. When configured to probe in this manner, it is necessary to configure a second Ethernet interface to be on the same subnet as the VRRP interface. This is because the VRRP interface cannot be used when it is in backup mode. The probes should be sent on this second interface. The second interface will have the other VRRP router as its gateway. The routing table should be configured to direct packets for the probe address to the desired interface.

every n seconds when in Backup state
The interval between successive probe attempts when the interface is in Backup state.

every n seconds when in Master state
The interval between successive probe attempts when the interface is in Master state.

Adjust priority n dir after x probe failures
These parameter control by how much and in which direction the VRRP priority is adjusted when the specified number of probes have failed.

Reset probe failure count after n probe successes
The number of consecutive successful probes that are required before the current failure count is reset to 0.

Use interface x,y over which to send probe
These parameters can be used to override the routing code and force the probe packets to be sent out of a specific interface.

Get the source IP address from interface x,y
These parameters can be used to the probe packets have the source IP address from a specific interface rather than the interface over which it is being transmitted.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eth	n	vrrpid	0 – 255	VRRP Group ID
eth	n	vrrpprio	0 - 255	VRRP Priority
eth	n	vboostprio	0 - 255	Boost the priority by n for s seconds after switching to the MASTER state
eth	n	vboostsecs	Integer	Boost the priority by n for s seconds after switching to the MASTER state
eth	n	vprobemode	off, TCP, ICMP	Send p probe to IP address a.b.c.d TCP port n
eth	n	vprobeip	IP Address	Send p probe to IP address a.b.c.d TCP port n
eth	n	vprobeport	0 – 65535	Send p probe to IP address a.b.c.d TCP port n
eth	n	vprobebackint	0 - 32767	every n seconds when in Backup state
eth	n	vprobemastint	0 - 32767	every n seconds when in Master state
eth	n	vprobeadj	0 - 255	Adjust priority n dir after x probe failures
eth	n	vprobeadjup	0 = down 1 = up	Adjust priority n dir after x probe failures
eth	n	vprobefailcnt	0 – 255	Adjust priority n dir after x probe failures

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eth	n	vprobesuccesscnt	0 - 255	Reset probe failure count after n probe successes
eth	n	vprobeent	Auto, ETH, PPP	Use interface x,y over which to send probe
eth	n	vprobeadd	Integer	Use interface x,y over which to send probe
eth	n	vprobeipent	Auto, ETH, PPP	Get the source IP address from interface x,y
eth	n	vprobeipadd	Integer	Get the source IP address from interface x,y

Logical Ethernet Interfaces

Configuration – Network> Interfaces > Ethernet > Logical Ethernet Interfaces

The logical Ethernet interfaces are virtual Ethernet interfaces. They can be configured as per the standard Ethernet interfaces except for the Speed and Duplex settings which require a physical interface.

Logical Ethernet interfaces can be used for assigning extra IP addresses to the router on the same or an alternate subnet using the same physical Ethernet connection.

Logical Ethernet interfaces can also be used for bridging features (such as used in a Wi-Fi configuration) where it is desirable to not use a physical interface for the bridging.

MAC Filtering

Configuration – Network> Interfaces> Ethernet > MAC Filtering

Ethernet MAC filtering can be used to restrict which Ethernet devices can send packets to the router. If MAC filtering is enabled on an Ethernet interface, only Ethernet packets with a source MAC address that is configured in the MAC Filter table will be allowed. If the source MAC address is not in the MAC Filter table, the packet will dropped.

Enable MAC filtering on Ethernet interfaces
Enable MAC filtering on a specific Ethernet interface.

MAC Address
The Ethernet source MAC address to allow. It is possible to allow a range of MAC addresses by configuring only the significant part of the MAC address. E.g. “00:04:2d” will allow all Ethernet packets with a source MAC address starting with “00:04:2d”.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eth	n	macfilt	on, off	Enable MAC filtering on Ethernet interfaces
macfilt	n	mac	MAC address with no separators. Partial MAC address are allowed.	MAC Address

MAC Bridging

Configuration – Network> Interfaces> MAC Bridging

The Ethernet MAC bridge function will create an Ethernet bridge between two physically separate Ethernet networks. It is possible to allow bridging over DSL, W-Wan, ISDN and PSTN connections but note that the only restriction on the traffic sent across the link is done via MAC address filtering and that all Ethernet traffic will be bridged, no firewall restrictions are applied to this traffic.

Once the bridge has been configured, the MAC addresses to bridge need to be configured in the MAC bridge table.

Enable
Enable MAC bridging on the Ethernet interface.

Forward to IP address
The IP address of the remote router to which the Ethernet packets will be bridged to.

Port
The TCP port that the remote router is listening on.

Listen on Port
The TCP port that the router will listen on for incoming bridged packet from the remote router.

MAC Address
The Ethernet destination MAC address of packets to be bridged. It is possible to allow a range of MAC addresses by configuring only the significant part of the MAC address. E.g. “00042d” will allow all Ethernet packets with a source MAC address starting with “00:04:2d”.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eth	n	srcbhost	IP Address	Forward to IP address
eth	n	srchport	0 – 65535	Port
eth	n	srcblistenport	0 - 65535	Listen on Port
bridgemac	n	mac	MAC address with no separators. Partial MAC address are allowed.	MAC Address

Spanning Tree Protocols

Configuration – Network> Interfaces > Ethernet > Spanning Tree Protocols

The Rapid Spanning Tree Protocol (RSTP) is a layer 2 protocol which ensures a loop free topology on a switched or bridged LAN whilst allowing redundant physical links between switches. When enabled, the TransPort device will use RSTP but this is backwards compatible with STP.

RSTP will not be enabled if the router is in "Port Isolate" mode. If an Ethernet interface is configured with a hub group, RSTP will be disabled on that interface.

Enable RSTP
Enables RSTP on the router.

Priority
Sets the RSTP priority.

Group
Sets the RSTP group that the router is in.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
stp	0	enable	on, off	Enable RSTP
stp	0	prio	0 – 65535	Priority
stp	0	group	-	Group
stp	0	debug	0, 1	Not available on the WEB interface.

Port status

To view the status of RSTP/STP on a router's Ethernet ports, the following commands can be used.

```
stp show
Port 0, Designated, Forwarding ctrl2:0x6
Port 1, Backup, Discarding ctrl2:0x1
Port 2, Backup, Discarding ctrl2:0x1
Port 3, Disabled, Discarding ctrl2:0x1
```

The port roles are

Disabled	There is nothing physically connected to this Ethernet port.
Root	A forwarding port that has been elected for the spanning-tree topology, towards the root bridge.
Designated	A forwarding port for every LAN segment, away from the root bridge.
Alternate	An alternate path to the root bridge. This path is different than using the root port.
Backup	A backup/redundant path to a segment where another bridge port already connects.

The STP port states are:

Disabled	The port is not functioning and cannot send or receive data.

Listening	The port is sending and receiving BPDU's and participates in the election process of the root bridge. Ethernet frames are discarded.
Learning	The port does not yet forward frames but it does learn source addresses from frames received and adds them to the MAC address table.
Forwarding	The port receiving and sending data, normal operation. STP still monitors incoming BPDU's that would indicate it should return to the blocking state to prevent a loop.
locking	A port that would cause a switching loop, no user data is sent or received but it may go into forwarding mode if the other links in use were to fail and the spanning tree algorithm determines the port may transition to the forwarding state. BPDU data is still received in blocking state.

The RSTP port states are

Learning	The port does not yet forward frames but it does learn source addresses from frames received and adds them to the MAC address table. The port processes BPDU's.
Forwarding	The port receiving and sending data, normal operation. STP still monitors incoming BPDU's that would indicate it should return to the blocking state to prevent a loop.
Discarding	A port that would cause a switching loop, no user data is sent or received but it may go into forwarding mode if the other links in use were to fail and the spanning tree algorithm determines the port may transition to the forwarding state. BPDU data is still received in blocking state.

VLANs

Configuration – Network> Interfaces> VLANS

VLANs (Virtual LANs) facilitate splitting a single physical LAN into separate Virtual LANs. This is useful for security reasons, and will also help cut down on broadcast traffic on the LAN.

Enable VLAN support on Ethernet interfaces
Enables VLAN support on the Ethernet interface.

VLAN ID
The ID of the Virtual LAN. This parameter is used in the TCP header to identify the destination VLAN for the packet.

Ethernet Interface
The Ethernet port that will tag the outgoing packets. Packets sent from this interface will have VLAN tagging applied.

IP Address
The destination IP address. This parameter is optional. If configured, only packets destined for this IP address will have VLAN tagging applied.

Mask
The destination IP subnet mask. This parameter is optional. If configured, only packets destined for this IP subnet mask will have VLAN tagging applied.

Source IP Address
The source IP address. This parameter is optional. If configured, only packets from this IP address will have VLAN tagging applied.

Source Mask
The source IP subnet mask. This parameter is optional. If configured, only packets from this IP subnet mask will have VLAN tagging applied.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eth	n	vlan	on, off	Enable VLAN support on Ethernet interfaces
vlan	n	vlanid	0 - 4095	VLAN ID
vlan	n	ethctx	Integer	Ethernet Interface
vlan	n	ipaddr	IP Address	IP Address
vlan	n	mask	IP Mask	Mask
vlan	n	srcipaddr	IP Addess	Source IP Address
vlan	n	srcmask	IP Mask	Source Mask

Wi-Fi

Configuration – Network> Interfaces> Wi-Fi

This is the section of the web interface that contains the configuration options required in order to configure and enable the Wi-Fi features. The **Configuration - Network > Interfaces > Wi-Fi** page has the following options:

- Global Wi-Fi settings
- Wi-Fi n
- Rogue Scan

Global Wi-Fi settings

Configuration – Network> Interfaces> Wi-Fi> Global Wi-Fi settings

Due to national restrictions on the channels available for use, the correct country should be selected from the drop down list to restrict the channels that are legal to use by the router. If required, a specific channel can be selected to over-ride the auto selection.

Country
Selecting a country from the drop down list will restrict the channels that the router will use. See table for more info on licensed channels.

Network Mode
Select your chosen mode of operation from the drop down list. The options are:

- A
- B / G

This parameter is not available on all routers.

Channel
Selecting "Auto" will allow the router to scan for a free channel within the range of legal channels for the selected country. It is possible to manually select a specific channel to use but care should be taken to ensure the selected channel is legal to use in the country.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
wifi	0	country	Country name	Country
wifi	0	chanmode	a / bg	Network Mode
wifi	0	channel	auto, 1 – 14	Channel

Below is a list of the countries that are currently supported:

Albania	Guatemala	Oman
Algeria	Honduras	Pakistan
Argentina	Hong Kong	Panama
Armenia	Hungary	Paraguay
Australia	Iceland	Peru
Austria	India	Philippines
Azerbaijan	Indonesia	Poland
Bahrain	Iran	Portugal
Belarus	Iraq	Puerto Rico
Belgium	Ireland	Qatar
Belize	Israel	Romania
Bolivia	Italy	Russia
Brazil	Jamaica	Saudi Arabia
Brunei	Japan	Singapore
Bulgaria	Jordan	Slovak Republic
Canada	Kazakhstan	Slovenia
Chile	Kenya	South Africa
China	North Korea	Spain
Colombia	South Korea	Sweden

Costa Rica	Kuwait	Switzerland
Croatia	Latvia	Syria
Cyprus	Lebanon	Taiwan
Czech Republic	Libya	Thailand
Denmark	Liechtenstein	Trinidad and Tobago
Dominican Republic	Lithuania	Tunisia
Ecuador	Luxembourg	Turkey
Egypt	Macau	U.A.E.
El Salvador	Macedonia	Ukraine
Estonia	Malaysia	United Kingdom
Faroe Islands	Mexico	United States
Finland	Monaco	Uruguay
France	Morocco	Uzbekistan
Georgia	Netherlands	Venezuela
Germany	New Zealand	Vietnam
Greece	Nicaragua	Yemen
	Norway	Zimbabwe

This table lists the licensed channels that will be used by the Digi when “Auto” is selected for the channel number.

Region	Channels
EMEA (excluding France)	1 - 13
France	10 - 13
Americas (excluding Mexico)	1 - 11
Mexico	1 - 8 Indoor, 9 - 11 outdoor
Israel	3 – 9
China	1 - 11
Japan	1 - 14

NOTE:
It is ILLEGAL to use restricted channels in certain countries.

Wi-Fi Hotspot

Configuration – Network> Interfaces> Wi-Fi> Global Wi-Fi settings> Wi-Fi Hotspots

This section enables the configuration of the global parameters that are applicable if using any Wi-Fi node as a hotspot.

Enable Wi-Fi Hotspot on

Click the checkbox to enable Wi-Fi Hotspot support on a particular Wi-Fi node.

Splashscreen filename
This selects an ASP web file that will be presented to the client's internet browser when they connect for the first time.

Each client can connect for h hrs m mins
The amount of time that a Wi-Fi client can use the Wi-Fi hotspot before having to re-authenticate.

Hotspot Exceptions
It is possible to configure a number of web locations for which authentication is not required. These allow the splashscreen to access these locations in order to display them to the client when authenticating.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
wifinode	n	hotspot	on, off	Enable Wi-Fi Hotspot on
wifi	0	hotspot_fname	Filename	Splashscreen filename
wifi	0	hotspot_lifetime	Integer	Each client can connect for h hrs m mins The CLI value is entered in seconds only.
hshosts	n	host	Hostname	Hotspot Exceptions

Wi-Fi Filtering

Configuration – Network> Interfaces> Wi-Fi> Global Wi-Fi settings> Wi-Fi Filtering

You can restrict access to the router via Wi-Fi. When the filtering is enabled, only MAC addresses configured in the table will be allowed to connect to the router.

Enable Wi-Fi filtering
Enable Wi-Fi filtering so that only clients who have their Wi-Fi MAC address configured in the MAC address table will be allowed to connect.

MAC Address
MAC addresses of Wi-Fi client that you wish to allow access to.
A valid MAC address has the format: 11:22:33:44:55:66. When entering this parameter, omit the ':' separators. For example 112233445566

NOTE:
Carefully review settings before applying changes. Incorrect settings can make the TransPort device inaccessible from the Wi-Fi network.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
wifi	0	macfilter	on/off	Enable Wi-Fi filtering
wififilt	n	mac	MAC address with no separators	MAC Address

Entity	Instance	Parameter	Values	Equivalent Web Parameter
			e.g. 112233445566	

Wi-Fi n

Configuration – Network> Interfaces> Wi-Fi> Wi-Fi n

When a Wi-Fi interface is configured to be an Access Point, an SSID must be configured in order for a Wi-Fi interface to operate.

In order to forward packets to and from a Wi-Fi interface, it must be bridged to a configured Ethernet interface. The Wi-Fi interface and Ethernet interface must be in the same Bridge instance.

If a DHCP server is required to run on the Wi-Fi interface, the DHCP server instance corresponding bridged Ethernet interface should be configured.

In some cases it may be necessary to bridge multiple Ethernet instances to a single Wi-Fi instance. If this is required, only one Ethernet instances is should be configured.

Enable this Wi-Fi interface
The Wi-Fi interface can be enabled or disabled.

Description
This parameter allows you to enter a descriptive name for the Wi-Fi interface to make it easier to identify.

SSID
When the Wi-Fi interface is configured to be an Access Point, this is the SSID that will be advertised to the Wi-Fi clients to.
When the Wi-Fi interface is configured to be a Client, this is the SSID of the Access Point you wish to connect to.

Mode
The Wi-Fi interface can be run in various modes. The options are:

- Access Point
- Client
- Rogue Detection (Scan for unauthorised Access Points)

This Wi-Fi interface is a member of Bridge instance n and therefore bridged to the following interfaces
When the Wi-Fi interface is configured to be an Access Point, in order to forward packets to and from the Wi-Fi interface it must be bridged with an Ethernet interface using a Bridge instance.

Interface
The interfaces that are currently members of the selected Bridge instance. Note that multiple Wi-Fi interfaces can be members of the same Bridge instance.

Link this Wi-Fi client interface with Ethernet n
When the Wi-Fi interface is configured to be a client, it must be bridged to a particular Ethernet interface.

This Wi-Fi rogue scanner will use Ethernet n
When the Wi-Fi interface is configured to be a rogue scanner, it will use the selected Ethernet interface.

Hide SSID
When enabled, the SSID will not be included in the beacon messages transmitted by the Wi-Fi interface when in Access Point mode. This means that Wi-Fi clients will not be able to auto-detect the Access Point.

Isolation
When enabled, connected Wi-Fi clients will not be able to communicate with other Wi-Fi clients or Ethernet hosts connected to this AP.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
wifinode	0	enabled	on, off	Enable this Wi-Fi interface
wifinode	0	descr	String	Description
wifinode	0	ssid	String up to 32 characters	SSID
wifinode	0	mode	ap, client, rogue	Mode
wifinode	o	bridge_inst	0 - 3	This Wi-Fi interface is a member of Bridge instance n and therefore bridged to the following interfaces
eth	n	bridge_inst	0 – 3	Interface
eth	n	wificli	On/Off	Link this Wi-Fi client interface with Ethernet n
eth	n	wificli_add	Integer	Link this Wi-Fi client interface with Ethernet n
wifinode	0	broadcastssid	On/ Off	Hide SSID
wifinode	0	isolation	On/Off	Enable station isolation
wifinode	0	identity		EAP authentication server identity
wifinode	0	sslcli_add		SSL client configuration
wifinode	0	eap_tls	On/Off	
wifinode	0	eap_peap	On/Off	

Wi-Fi Security

Configuration – Network> Interfaces> Wi-Fi> Wi-Fi n> Wi-Fi Security

This section is used to configure the security settings for the Wi-Fi interface.

If using multiple Wi-Fi interfaces at the same time then the interfaces will need to use the same security settings (except for the pre-shared key (PSK)). The only alternative is that the Wi-Fi is be used with no security.

Use the following security on this Wi-Fi interface
Selects the security that is used on this Wi-Fi interface. The options are:

- None
- WEP
- WPA-PSK (also known as “WPA Personal”)
- WPA2-PSK (also known as “WPA2 Personal”)
- WPA-RADIUS (also known as “WPA Enterprise”)
- WPA2-RADIUS (also known as “WPA2 Enterprise”)

WEP Settings
The various WEP security settings for both Access Point and Client modes.

WEP Key size
The key size to use.

WEP Key index
The WEP key index number. This needs to match the index selected on the connecting Wi-Fi clients or Access Points that this router wishes to connect to.

WEP Key / Confirm WEP Key
If the WEP key size is 64 bits, the key should be 5 characters long. If the WEP key size is 128 bits, the key should be 13 characters long.

WPA-PSK / WPA2-PSK
The various WPA-PSK / WPA2-PSK security settings for both Access Point and Client modes.

WPA Encryption
The encryption algorithm to use. The options are:

- TKIP
- AES (CCMP)

WPA pre-shared key / Confirm WPA pre-shared key
The pre-shared key (PSK) to use. It must be between 8 and 63 characters long.

WPA-RADIUS / WPA2-RADIUS
The various WPA-RADIUS / WPA2- RADIUS security settings for both Access Point and Client modes.

WPA Encryption
The encryption algorithm to use. The options are:

- TKIP
- AES (CCMP)

RADIUS NAS ID
NAS ID of the RADIUS server.

RADIUS Server IP Address
IP address of the RADIUS server

RADIUS Server Password / Confirm RADIUS Server Password
The password of the RADIUS server.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
wifinode	0	security	none wep wpapsk	Use the following security on this Wi-Fi interface

Entity	Instance	Parameter	Values	Equivalent Web Parameter
			wpa2psk wparadius wpa2radius	
wifinode	0	weptype	open, sharedkey	Not available on the WEB.
wifinode	0	wepkeylen	64, 128	WEP Key size
wifinode	0	wepkeyindex	1 - 4	WEP Key index
wifinode	0	wpatype	tkip, aes	WPA Encryption
wifinode	0	sharedkey	text	WEP Key/WPA pre-shared key
radcli	n*	nasid	String	RADIUS NAS ID
radcli	n*	server	IP Address	RADIUS Server IP Address
radcli	n*	password	String	RADIUS Server Password

* The Wi-Fi interfaces each use a fixed RADIUS client, e.g.,

- Wi-Fi 0 uses radcli 1
- Wi-Fi 1 uses radcli 2
- Wi-Fi 2 uses radcli 3 and so on.

The table below details the authentication and encryption algorithms and the CLI commands needed to configure them:

Network Authentication	Data Encryption	CLI Commands
Open	Disabled	wifinode 0 security none
Shared	Disabled	Not supported
Open	WEP	wifinode 0 security wep wifinode 0 weptype open wifinode 0 wepkeylen <64 | 128> wifinode 0 wepkeyindex <1..4> wifinode 0 sharedkey <5 or 13 char key>
Shared	WEP	wifinode 0 security wep wifinode 0 weptype sharedkey wifinode 0 wepkeylen <64 | 128> wifinode 0 wepkeyindex <1..4> wifinode 0 sharedkey <5 or 13 char key>
WPA	TKIP	wifinode 0 security wparadius wifinode 0 wpatype tkip wifinode 0 radiuscfg 1
WPA2	TKIP	wifinode 0 security wpa2radius

Network Authentication	Data Encryption	CLI Commands
		wifinode 0 wpatype tkip wifinode 0 radiuscfg 1
WPA-PSK	TKIP	wifinode 0 security wpapsk wifinode 0 wpatype tkip wifinode 0 sharedkey <8..63 char key>
WPA2-PSK	TKIP	wifinode 0 security wpa2psk wifinode 0 wpatype tkip wifinode 0 sharedkey <8..63 char key>
WPA	AES	wifinode 0 security wparadius wifinode 0 wpatype aes wifinode 0 radiuscfg 1
WPA2	AES	wifinode 0 security wpa2radius wifinode 0 wpatype aes wifinode 0 radiuscfg 1
WPA-PSK	AES	wifinode 0 security wpapsk wifinode 0 wpatype aes wifinode 0 sharedkey <8..63 char key>
WPA2-PSK	AES	wifinode 0 security wpa2psk wifinode 0 wpatype aes wifinode 0 sharedkey <8..63 char key>

Rogue Scan

Configuration – Network> Interfaces> Wi-Fi> Rogue Scan

In Rogue Scan mode, the router will perform a scan of the Wi-Fi channels and will report what Wi-Fi Access Points it detects. This feature can be used to detect unauthorised Access Points that might be trying to get unsuspecting Wi-Fi clients to connect them.

When an authorised Access Point is detected, an event log entry is created and an alarm (e.g. email, SMS, SNMP Trap) can be triggered.

It is possible to configure a list of the MAC addresses of the authorised Access Points that will not be reported when detected.

MAC Address
The MAC address of an authorised Access Point.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter

Entity	Instance	Parameter	Values	Equivalent Web Parameter
macrogue	n	mac	MAC address with no separators *e.g.* 112233445566	MAC Address

Mobile

Configuration – Network > Interfaces > Mobile

The ***Configuration – Network > Interfaces > Mobile*** page has the following options:

- Mobile Settings
- SIM Selection
- Advanced

Wireless WAN functionality is only available on models that are fitted with a wireless WAN module ,such as CDMA, GPRS, 3G, HSPA etc. This module is connected to one of the ASY ports (and USB controller on some models) and is controlled by the router using "AT" commands (in the same way as a modem). Any further references to W-WAN technologies such as CDMA, GPRS, 3G etc. will be referred to as GPRS, GSM, 3G or simply 'wireless' networks.

W-WAN modules provide always-on wireless data connectively over the GSM network at speeds of up to 7.2Mbps. This means that the unit can be used in situations where no ISDN or xDSL service connection is available. In addition, wireless can be used to send or receive SMS alert messages (as an alternative to emails for issuing remote alert messages or for automating remote configuration of deployed units).

Before attempting to connect to a wireless service, you need to set several parameters specific to your mobile network operator. It will be useful to have the following information to hand:

- The assigned APN (Access Point Name)
- PIN Number for your SIM card (if any)
- Username and password

Once the W-WAN router is correctly configured, check to see if it has obtained an IP address from the network by navigating to the Diagnostics - Status > PPP > PPP x page (where x is either 1 or 3 depending on the model) and checking the IP address parameter. (It should contain an IP address other than 0.0.0.0 or 1.2.3.4).

Additionally, check that the SIM is working correctly and also check the signal strength by navigating to the Status > Mobile page.

SIM:

Select a SIM to configure. SIM 1 relates to the SIM card fitted to the slot marked SIM 1 on the router's front panel. SIM 2 relates to the SIM card fitted to the slot marked SIM 2.

Note:

When using a single SIM card only, the default action is for the router to use PPP 1 as the mobile interface.

To configure 2 SIM's for fail-over browse to ***Configuration - Network > Interfaces > Mobile > SIM Selection*** to launch the Dual SIM wizard.

Mobile Settings

Configuration – Network > Interfaces > Mobile> Mobile Settings

Select the service plan and connection settings used in connecting to the mobile network.

Mobile Service Provider Settings

The ***Configuration – Network > Interfaces > Mobile > Mobile Settings*** option opens to show the following parameters:-

Service Plan / APN:
Enter the APN (Access Point Name) given by the service provider.

Use backup APN
Tick to enable this option then enter the backup APN in the free text field
e.g. “your.apn”
This parameter may be used to specify an alternative service APN for use in the event that the unit cannot connect using the primary APN specified by the APN parameter. The unit will only use this APN if the primary APN fails and the Use backup APN parameter is enabled.

Retry the main APN after n minutes
If the Use backup APN parameter is enabled, this parameter is used to define how long the unit will use the backup APN before attempting to revert to the primary APN.

SIM PIN:
Some SIM cards are locked with a Personal Identification Number (PIN) code to prevent misuse if they are lost or stolen. The GSM operator should be able to confirm if the SIM requires a PIN code.
If you enter a PIN code in this field, the unit will try to unlock the SIM before attempting to connect to the network.

Confirm SIM PIN:
Enter the PIN again in this field to confirm it.

Username: (Optional)
Some APNs require a username and password for the PPP connection. These are not always pre-defined i.e. any “made-up” username or password will suffice.

Password: (Optional)
Enter the password for the PPP connection.

Confirm Password:
Enter the password again in this field to confirm it.

Related CLI Commands

SIM 1 (PPP 1)

Entity	Instance	Parameter	Values	Equivalent Web Parameter
modemcc	0	apn	Free text field	Service Plan / APN:
modemcc	0	usebuapn	on/off	Checkbox (Use Backup APN)
modemcc	0	buapn	Free text field	Use backup APN
modemcc	0	pin	SIM PIN number	SIM PIN:/Confirm SIM PIN
ppp	1	username	Free text field	Username:
ppp	1	password	Free text field	Password:/Confirm Password

SIM 2 (PPP 1)

Entity	Instance	Parameter	Values	Equivalent Web Parameter
modemcc	0	Apn_2	Free text field	Service Plan / APN:
modemcc	0	Usebuapn_2	on/off	Checkbox (Use Backup APN)
modemcc	0	Buapn_2	Free text field	Use backup APN
modemcc	0	Pin_2	SIM PIN number	SIM PIN:/Confirm SIM PIN
ppp	1	username	Free text field	Username:
ppp	1	password	Free text field	Password:/Confirm Password

Mobile Connection Settings

Re-establish connection when no data is received for a period of time.
This checkbox opens to show the following parameters:-

Inactivity Timeout: h hrs m mins s seconds
This parameter specifies the amount of time the unit will wait without receiving any PPP packets before disconnecting. An inactivity timeout reset with each received PPP packet.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	1	rxtimeout	0 – 86400 (seconds)	Re-establish connection when no data is received for a period of time. Inactivity Timeout: h hrs m mins s seconds

Mobile Network Settings

Enable NAT on this interface
This parameter is used to enable or disable IP Network Address Translation (NAT) on the mobile interface.
This checkbox opens to show the following options:-

IP Address:
Enable standard Network Address Translation (NAT).

IP address and Port:
Enable Network Address and Port Translation (NAPT).

Enable IPsec on this interface
This parameter is used to enable or disable IPSec processing on the mobile interface. If enabled, packets sent or received on this interface must pass through the IPSec code before being transmitted. IPSec may drop the packet, pass it unchanged, or encrypt and encapsulate within an IPSec packet.
This checkbox opens to show the following parameters:-

Keep Security Associations (SAs) when this Mobile interface is disconnected
This checkbox will configure the router to keep any existing IKE and IPsec associations should the link drop. This is usually applied on head-end routers with fixed IP addresses.

Use interface X, Y for the source IP address of IPsec packets

By default, the source IP address for an IPSec Eroute will be the IP address of the interface on which IPSec was enabled. By setting this parameter to either a PPP or Ethernet interface, the source IP address used by IPSec will match that of the Ethernet or PPP interface specified.

Enable the firewall on this interface
The Firewall parameter is used to enable or disable the Firewall script processing for the mobile interface.

Note:
If the firewall is enabled on an interface and with the absence of any firewall rules, the default action is to block ALL traffic.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	1	do_nat	1	Enable NAT on this interface IP Address
ppp	1	do_nat	2	Enable NAT on this interface IP Address and Port
ppp	1	ipsec	1	Enable IPsec on this interface
ppp	1	ipsec	2	Keep Security Associations (SAs) when this Mobile interface is disconnected
ppp	1	ipsecent	blank,ETH,PPP	Use interface X, Y for the source IP address of IPsec packets x = Interface type
ppp	1	ipsecadd	0 - 255	Use interface X, Y for the source IP address of IPsec packets y = interface number
ppp	1	firewall	on/off	Enable the firewall on this interface

SIM Selection

Configuration – Network > Interfaces > Mobile > SIM Selection

This section allows you to launch the Dual SIM wizard for failing over from 1 SIM to another.

Click here to launch the Dual SIM wizard
Click the hyperlink to launch the Dual SIM wizard.

CDMA Provisioning

If the router was not supplied pre-provisioned, obtain the following details from the Service Provider:

a 15 digit IMSI (International Mobile Subscriber Identity)

an NAI (Network Access Identifier)

an NAI password

Once these details have been obtained, it is possible to provision the CDMA module by inserting those details into the 'Automatic Provisioning' section of this web page and clicking on the Start button.

See Quick Note 25 – "CDMA Provisioning on a Digi TransPort Router" for example configuration.

Automatic Provisioning

If required, enter the MSL/PTN/MSID parameters before clicking Start

MSL:
Master subsidy lock (MSL) code. Obtain this from the mobile operator.
PTN:
Personal Telephone Number. Obtain this from the mobile operator.
MSID:
Mobile Station Identifier. Obtain this from the mobile operator.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
provision	0	string1	No data input required	MSL
provision	0	String2	No data input required	PTN
provision	0	String3	No data input required	MSID

Manual Provisioning

Manual provisioning should only be attempted by experienced technical personnel who have obtained all the required information from the mobile operator. Technical personnel with previous provisioning experience should not require these parameters explaining.

MSL:
Master subsidy lock (MSL) code. Obtain this from the mobile operator.
MDN:
Personal Telephone Number. Obtain this from the mobile operator.
MIN/MSID:
Mobile Station Identifier. Obtain this from the mobile operator.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
provision	0	String4	Free text field	MSL
provision	0	String5	Free text field	PTN
provision	0	String6	Free text field	MIN/MSID

Mobile IP settings

Configuration – Network > Interfaces > Mobile> Mobile IP settings

Mobile IP profile number:
Enter the Mobile IP profile number
Network Access ID (NAI):
Enter the Network Access ID
MIP Home Address:
Enter the MIP Home Address
Primary Home Agent:
Enter the Primary Home Agent
Secondary Home Agent:
Enter the Secondary Home Agent
HA shared secret: 0xn (Hex strings must start 0x)
Enter the HA shared secret
AAA shared secret: 0xn (Hex strings must start 0x)
Enter the AAA shared secret
HA SPI:
Enter the HA SPI
AAA SPI:
Enter the AAA SPI
Enable Reverse tunnelling:
Enable Reverse tunnelling if required.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
provision	0	String7	1	Mobile IP profile number:
provision	0	String8	Free text field	Network Access ID (NAI):
provision	0	String9	Free text field	MIP Home Address:
provision	0	String10	Free text field	Primary Home Agent:
provision	0	String11	Free text field	Secondary Home Agent:
provision	0	String12	Hex string	HA shared secret: 0xn (Hex strings must start 0x)
provision	0	String13	Hex string	AAA shared secret: 0xn (Hex strings must start 0x)
provision	0	String14	Free text field	HA SPI:
provision	0	String15	Free text field	AAA SPI:
provision	0	String16	Free text field	Enable Reverse tunneling:

PRL Update

The Preferred Roaming List is a list of bands and channels in order of preference which the CDMA module uses when it attempts to locate and connect to a cell system. If the router is having problems with CDMA reception, it would be beneficial to update the PRL information.

MSL:

Master subsidy lock (MSL) code. Obtain this from the mobile operator.

PRL filename:
Preferred Roaming List file name. Obtain this from the mobile operator.

Note: With the exception of older Sierra Wireless modules, PRL update on both the Verizon and Sprint networks is carried out over the air (OTA). Manual PRL update using a PRL file is not available. To initiate automatic over the air PRL update, click the **Start** button. Please note that PRL update is normally carried out as part of automatic provisioning on both Sprint and Verizon.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
provision	0	string1	Free text field	MSL
provision	0	string20	Free text field	PRL Filename

Advanced

Configuration – Network > Interfaces > Mobile> Advanced

SIM PUK:
(Optional) If known, the SIM PUK code can be entered in these fields. If the router detects that a PUK is required due to a locked SIM, this number will be sent to the SIM. A SIM PIN must also be configured for the PUK parameter to take effect.

Confirm SIM PUK:
Enter the PUK code again in this field to confirm it.

Initialisation string <n>:
These parameters (Initialisation string 1, Initialisation string 2, Initialisation string 3) allow you to specify a number of command strings that are sent to the wireless module each time a wireless connection is attempted. These can be used to set non-standard wireless operating modes.

Each string is prefixed with the characters “AT” before being sent to the wireless module and they are sent to the wireless module in the order specified until an empty string is encountered. For example, Initialisation string 3 will not be sent unless Initialisation string 1 and Initialisation string 2 are both specified. Initialisation strings are not normally required for most applications as the unit will normally be pre-configured for correct operation with most networks.

Hang-up string:
In a typical wireless application the connection to the network is “always on” and under normal circumstances it is not necessary to hang-up the wireless module. Under certain circumstances however, the router may use the “ATH” command to try and disconnect the wireless module from the network, e.g. if an incorrect APN has been specified and the module is unable to attach to the network correctly.

This parameter allows you to specify an alternative hang-up string that is sent to the wireless module when disconnecting a call. As with the Initialisation strings, it is not necessary to include the “AT” as this is inserted automatically by the router

Post Hang-up string:
This parameter allows you to specify additional “AT” commands that is sent to the wireless module after it has been disconnected. As with the Initialisation strings, it is not necessary to include the “AT” as this is inserted automatically by the router.

Wait n seconds between hanging up and allowing another call
This parameter is used to specify the length of time (in n seconds) that the router will wait after hanging-up the wireless module before initiating another call attempt.

Wait n seconds between attachment attempts
The number of seconds between network attachment attempts, some networks require 60 seconds between attempts to attach to the wireless network.

Reset the module after n unsuccessful connection attempts The router will normally make multiple attempts to connect to the wireless network in the event that the signal is lost. In some cases, this can result in a "lock-up" situation where the wireless network is unable to attach the wireless device due to the multiple attempts. This parameter specifies the number of attempts at connection that the unit should make before power cycling the internal wireless module. Power cycling the wireless module forces it to re-register and reattach to the network. The default setting of 10 is the recommended value. Setting this parameter to 0 will prevent the router from power cycling the wireless module if it cannot obtain an IP address.

Reset the module after n unsuccessful status retrieval attempts
The router will periodically collect status information from the internal wireless module. This information, which may be viewed on the ***Management - Network Status > Interfaces > Mobile*** web page, includes details of the signal strength and network attachment status. As a safeguard against problems communicating with the wireless module, the Status retries parameter may be used to specify the number of unsuccessful attempts to retrieve status information from the wireless module before power cycling it. The default setting of 30 is the recommended value. Setting this parameter to 0 will prevent the router from power cycling the wireless module if it cannot read the wireless status information.

Create a signal strength event every n minutes
When configured, the signal strength will be written to the eventlog every *n* minutes.

If registration is lost for 5 minutes
This parameter controls whether the unit will power cycle the wireless module after the network registration has been lost for 5 minutes. Setting this parameter to "Do not reset the module" will never recycle the wireless module, setting to "reset the module if GSM registration is lost" will power cycle the module after 5 minutes loss of GSM registration, and setting to "reset the module if GSM registration is lost" will power cycle the module after 5 minutes loss of GPRS, 3G or HSPA registration.

Preferred System:

This parameter controls which mobile technology will be used as the preferred system (2G/3G). When set to "Auto" the wireless module will choose the fastest technology available. For GSM: When set to "GSM", the wireless module will try GSM (GPRS/EDGE) technology first. When set to "WCDMA", the wireless module will try WCDMA (UMTS/HSPA) technology first. For CDMA: Select CDMA for 2G (1xRTT) or EVDO for 3G.

Related CLI Commands - SIM Slot 1 (PPP 1)

Entity	Instance	Parameter	Values	Equivalent Web Parameter
modemcc	0	puk	sim puk code	SIM PUK/Confirm SIM PUK
modemcc	0	init_str	Free text field	Initialisation string 1
modemcc	0	init_str1	Free text field	Initialisation string 2
modemcc	0	init_str2	Free text field	Initialisation string 3
modemcc	0	hang_str	Free text field	Hang-up string:
modemcc	0	posthang_str	Free text field	Post Hang-up string:
modemcc	0	intercall_idle	0 - 2147483647	Wait n seconds between

Entity	Instance	Parameter	Values	Equivalent Web Parameter
				hanging up and allowing another call
modemcc	0	att_interval	0 - 2147483647	Wait n seconds between attachment attempts
modemcc	0	link_retries	0 - 2147483647	Reset the module after n unsuccessful connection attempts
modemcc	0	stat_retries	0 - 2147483647	Reset the module after n unsuccessful status retrieval attempts
modemcc	0	ss_interval	0 - 2147483647	Create a signal strength event every n minutes
modemcc	0	check_reg	0,1,2	If registration is lost for 5 minutes 0 = do not reset the module 1 = reset the module if the GSM registration is lost 2 = reset the module if the GPRS registration is lost
modemcc	0	psys	0,1,2	Preferred System 0 = Auto 1 = GSM 2 = WCDMA

Related CLI Commands - SIM Slot 2 (PPP 1)

Entity	Instance	Parameter	Values	Equivalent Web Parameter
modemcc	0	Puk_2	sim puk code	SIM PUK/Confirm SIM PUK
modemcc	0	init_str_2	Free text field	Initialisation string 1
modemcc	0	init_str1_2	Free text field	Initialisation string 2
modemcc	0	init_str2_2	Free text field	Initialisation string 3
modemcc	0	hang_str_2	Free text field	Hang-up string:
modemcc	0	posthang_str_2	Free text field	Post Hang-up string:
modemcc	0	intercall_idle_2	0 - 2147483647	Wait n seconds between hanging up and allowing another call
modemcc	0	att_interval_2	0 - 2147483647	Wait n seconds between attachment attempts
modemcc	0	link_retries_2	0 - 2147483647	Reset the module after n unsuccessful connection attempts
modemcc	0	stat_retries_2	0 - 2147483647	Reset the module after n unsuccessful status retrieval

Entity	Instance	Parameter	Values	Equivalent Web Parameter
				attempts
modemcc	0	ss_interval_2	0 - 2147483647	Create a signal strength event every n minutes
modemcc	0	check_reg_2	0,1,2	If registration is lost for 5 minutes 0 = do not reset the module 1 = reset the module if the GSM registration is lost 2 = reset the module if the GPRS registration is lost
modemcc	0	Psys_	0,1,2	Preferred System 0 = Auto 1 = GSM 2 = WCDMA

Mobile Network Settings

Metric:
This parameter specifies the connected metric of the mobile interface. The default metric of a connected interface is 1. By allowing the interface to have a higher value (lower priority), static routes can take preference to interfaces. For normal operation, leave this value unchanged.

Generate Heartbeats on this interface
Heartbeat packets are UDP packets that contain status information about the unit that may be used to locate a remote unit's current dynamic IP address.
This checkbox opens to show the following parameters:-

Send Heartbeat messages to IP address a.b.c.d every h hrs m mins s secs
If these parameters are set to a non-zero value, the router will transmit "heartbeat" packets to the specified IP address/hostname at the specified interval.

Use interface x,y for the source IP address
This parameter allows the selection of the source interface for the UDP heartbeats. For example, it may be required to send the heartbeat packets down a VPN tunnel. And in order to match the corresponding subnets of the VPN, it might require changing the source IP to match an inside Ethernet interface.
For normal operation, using the mobile interface as the source IP address, leave this value unchanged.

Select transmit interface using the routing table
When enabled, the UDP heartbeats will choose the best route from the routing table. If disabled the exit interface will be interface on which the heartbeat is configured.

Include IMSI information in the Heartbeat message
When enabled, the heartbeat will include the IMSI of the wireless module.

Include GPS information in the Heartbeat message
When enabled, the heartbeat will include the GPS co-ordinates of the router.

Generate Ping packets on this interface
This section relates to monitoring pings which can be sent from the mobile interface. For more details refer to "Application Note 7 Wireless WAN problem Detection and Recovery".

This checkbox opens to show the following parameters:-

Send n byte pings to IP host a.b.c.d every h hrs m mins s secs
If this parameter is set, the router will automatically generate a "ping" of n size to the IP host specified (IP address or hostname) at the interval specified. Deleting the IP host value disables the monitoring ping facility.
This parameter in conjunction with "Reset the link if no response is received within s seconds" can be used to configure the unit to use a back-up interface automatically should there be a problem with this interface.

Note:
The **n** parameter specifies the PING size when using monitoring ping feature. The size indicates how large the ICMP packet should be excluding the size of the IP header.

Send pings every h hrs m mins s secs if ping responses are not being received
If this parameter is set, the router will use this value as the interval to ping at when more than one ping request sent out the PPP interface is outstanding. This should be set to a shorter interval than the above ping request interval so that the router may more quickly react to a broken PPP link.

Switch to sending pings to IP host a.b.c.d after n failures
This allows a for more reliable problem detection before fail over occurs by testing connectivity to 2 IP addresses/hostnames. If an IP address or host name is entered and the n parameter has a value greater than 0, when a ping failure is detected on the primary IP address, pings will be sent to this 2nd IP address/hostname. This is to ensure that if the main IP address becomes unavailable for any reason and stops responding to ICMP requests, the router will check another IP address before starting fail over procedures.

Ping responses are expected within n seconds
If this parameter is set to a non-zero value the unit will wait for the interval specified for a response from a PING request before applying the "**Send pings every h hrs m mins s secs if ping responses are not being received**". If this parameter is set to 0 (default), the time specified in the in "**Send n byte pings to IP host a.b.c.d every h hrs m mins s secs**" is allowed before applying the "**Send pings every h hrs m mins s secs if ping responses are not being received**".

Only send Pings when this interface is "In Service"
When enabled this parameter, ICMP echo requests will only be sent from this interface when it is in service. The default setting is off and ICMP echo requests are sent when the interface is in service and out of service.

New connections to resume with previous Ping interval
When enabled, this parameter controls the ping interval after the mobile interface has been de-activated and then re-activated. It sets the ping interval to the same interval in use when the mobile link last disconnected.

Reset the link if no response is received within s seconds
This parameter specifies an amount of time after which if no ping response has been received, the unit will terminate the mobile connection in an attempt to re-establish communications. Because by default the mobile link is always on, the unit will automatically attempt to re-establish a PPP connection that has been terminated.

Use the ETH 0 IP address as the source IP address

Enabling this parameter causes the unit to use the IP address of ETH0 (instead of the current IP address of the mobile interface), as the source address for the auto PING packets.

Note:
This parameter is useful if you want to send the monitoring pings down a VPN tunnel where the source IP address needs to match the LAN.

Defer sending pings if IP traffic is being received
When enabled, the timer configured in the "**Send n byte pings to IP host a.b.c.d every h hrs m mins s secs**" parameter will be reset if IP data is sent across the mobile link.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	1	metric	0 - 256	Metric
ppp	1	hrtbeatip	IP address	Send Heartbeat messages to IP address a.b.c.d every h hrs m mins s secs
ppp	1	hrtbeatint	0 – 2147483647 (seconds)	Send Heartbeat messages to IP address a.b.c.d every h hrs m mins s secs
ppp	1	hbipent	Default,PPP,Ethernet	Use interface x,y for the source IP address
ppp	1	hbipadd	number	Use interface x,y for the source IP address
ppp	1	hbroute	on/off	Select transmit interface using the routing table
ppp	1	hbimsi	on/off	Include IMSI information in the Heartbeat message
ppp	1	hbgps	on/off	Include GPS information in the Heartbeat message
ppp	1	pingsiz	number	Send n byte pings to IP host a.b.c.d every h hrs m mins s secs
ppp	1	pingip	hostname	Send n byte pings to IP host a.b.c.d every h hrs m mins s secs
ppp	1	pingint	0 – 2147483647 (seconds)	Send n byte pings to IP host a.b.c.d every h hrs m mins s secs
ppp	1	pingint2	0 – 2147483647 (seconds)	Send pings every h hrs m mins s secs if ping responses are not being received
ppp	1	pingip2	IP address	Switch to sending pings to IP host a.b.c.d after n failures

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	1	ip2count	number	Switch to sending pings to IP host a.b.c.d after n failures
ppp	1	pingresp	0 – 2147483647	Ping responses are expected within n seconds
ppp	1	pingis	on/off	Only send Pings when this interface is "In Service"
ppp	1	ping2cont	on/off	New connections to resume with previous Ping interval
ppp	1	pingdeact	0 - 2147483647	Reset the link if no response is received within s seconds
ppp	1	pingfreth0	on/off	Use the ETH 0 IP address as the source IP address
ppp	1	pingresetint	on/off	Defer sending pings if IP traffic is being received

SMS Settings

Configuration – Network > Interfaces > Mobile> SMS Settings

Mobile routers can be configured to send and receive SMS messages. The sending of SMS messages could for example be in conjunction with sending alarms and received messages for configuration changes, or status requests.

Poll for incoming SMS messages
This checkbox opens to show the following parameter:-

Every n minutes
This specifies the interval in minutes that the unit will wait in between checks for incoming SMS messages. Setting this interval to “0” turns off checking.

Enable command replies via SMS
This parameter enables or disables replies to SMS commands.

Concatenate replies
Normally an SMS message is limited to 160 characters. However, the ETSI standard specifies a way to allow a number of SMS messages to be linked together by the sender (in this case the router). This enables the router to reply with long responses to SMS commands of longer than 160 characters. The reply comes back as a series of linked SMS messages which the phone reassembles and displays as one big message.

Note:
The routers cannot handle received concatenated SMS messages, it can only transmit concatenated SMS messages

Use this SMS message centre number n instead of the network default
This setting is not usually required. It is the number of the SMS message center (sometimes referred to as the Service Centre Address), to be used to relay SMS messages or alarms. This number must include the international dialling code, e.g. 44 for the UK, but not the “+” prefix or leading 0’s, e.g. 44802000332. SMS alarms are generated when the SMS trigger

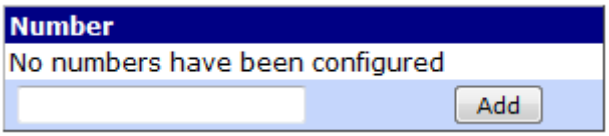
priority is greater than 0 and an event of this priority or higher occurs. SMS alarms may be configured using the ***Configuration - Alarms > Event Settings > SMS*** web page

If no number is specified it is possible that the unit will operate using the default message centre for the GSM service to which you have subscribed.

SMS access level:
The access level for SMS commands. The access level set here will need to match the level required by the command sent by SMS for the command to be accepted.

Use x as a command separator (default is CR)
This parameter specifies the character to be used to separate multiple command lines when a remote SMS sender is controlling the unit. The default separator is <CR> but some SMS capable devices are not equipped with <CR> keys so an additional means of separating multiple lines is required.

Allow CLI commands from the following SMS numbers.
You may specify up to 10 numbers. Specifying * permits commands from any SMS number. Numbers are applied in the following input box. Click 'Add' to submit



Related CLI Commands - SIM Slot 1 (PPP 1)

Entity	Instance	Parameter	Values	Equivalent Web Parameter
modemcc	0	sms_interval		Poll for incoming SMS messages:- Every n minutes
modemcc	0	sms_replies	on/off	Enable command replies via SMS
modemcc	0	sms_concat	Number 0 = off 10 = default when enabled	Concatenate replies
modemcc	0	sca	Free text field	Use this SMS message centre number n instead of the network default
modemcc	0	sms_access	0 = Super (default) 1 = High 2 = Medium 3 = Low 4 = None 5 = HighLow 6 = HighMedium 7 = CheckPar	SMS access level:
modemcc	0	sms_cmd_sep	Free text field	Use as a command separator (default is CR)

Entity	Instance	Parameter	Values	Equivalent Web Parameter
modemcc	0	sms_callerid	Mobile telephone number	Allow CLI commands from the following SMS numbers. (First SMS number)
modemcc	0	sms_callerid_1 to 9	Mobile telephone number	Allow CLI commands from the following SMS numbers. (additional SMS numbers 1 to 9)

Related CLI Commands - SIM Slot 2 (PPP 1)

Entity	Instance	Parameter	Values	Equivalent Web Parameter
modemcc	0	sms_interval_2		Poll for incoming SMS messages:- Every n minutes
modemcc	0	sms_replies_2	on/off	Enable command replies via SMS
modemcc	0	sms_concat_2	Number 0 = off 10 = default when enabled	Concatenate replies
modemcc	0	Sca_2	Free text field	Use this SMS message centre number n instead of the network default
modemcc	0	sms_access_2	0 = Super (default) 1 = High 2 = Medium 3 = Low 4 = None 5 = HighLow 6 = HighMedium 7 = CheckPar	SMS access level:
modemcc	0	sms_cmd_sep	Free text field	Use as a command separator (default is CR)
modemcc	0	sms_callerid	Mobile telephone number	Allow CLI commands from the following SMS numbers. (First SMS number)
modemcc	0	sms_callerid_1 to 9	Mobile telephone number	Allow CLI commands from the following SMS numbers. (additional SMS numbers 1 to 9)

DSL

Configuration – Network > Interfaces > DSL

The ***Configuration – Network > Interfaces > DSL*** page has the following options:

- PVC Configuration
- DSL Network Settings
- PVC Traffic Shaping
- Advanced

Router models incorporating a DSL broadband interface will include a configuration page having the title shown above. By default, the configuration in this section will be suitable for the majority of ADSL service providers in the UK. However, advanced users or users outside of the U.K. may wish or need to adjust some of the parameters.

Enable DSL
This checkbox gives the facility to enable or disable the use of DSL/ADSL functionality on the router.

Configure PVC
Select the required PVC instance from the drop-down selection box. Subsequent settings will apply to the selected instance (see below).

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eth	0	vdsl	OFF/ON	Link VDSL interface with Ethernet n

PVC Configuration

Configuration – Network > Interfaces > DSL> PVC Configuration

The PVC (Permanent virtual circuit) parameters are described here.

Enable this PVC
Tick the box to enable PVC settings

Encapsulation
This parameter is used to select the method of encapsulation to be used when transporting data over this APVC. The appropriate value can be selected from a drop list which includes the following options:

Option	Description
PPPoA VC-Mux	RFC 2364 VC-multiplexed PPP over AAL5
PPPoA LLC	RFC 2364 LLC encapsulated PPP over AAL5
PPPoE VC-Mux	RFC 2516 VC-multiplexed PPP over Ethernet
PPPoE LLC	RFC 2516 LLC encapsulated PPP over Ethernet
Bridged Ethernet VC-Mux	RFC 2684 VC-multiplexed bridged Ethernet
Bridged Ethernet LLC	RFC 2684 LLC encapsulated bridged Ethernet
Routed IP VC-Mux	RFC 1483 VC multiplexing routed IP over

Option	Description
	ATM
Routed IP LLC	RFC 1483 LLC encapsulated routed IP over ATM

To use PPPoA or PPPoE encapsulation, one of the available PPP instances must first be configured to use this APVC instance as its Layer 1 interface on the associated ***Configuration – Interfaces*** **>** ***PPP*** **>** ***PPP n*** **>** ***Advanced*** page.

VPI
This parameter is used to set the Virtual Path Identifier for this APVC in the range 0 - 255.

VCI
This parameter is used to set the Virtual Channel Identifier for this APVC in the range 0 - 65535.

Entity	Instance	Parameter	Values	Equivalent Web Parameter
apvc	0	vpi	0-255	VPI
apvc	0	vci	0-65535	VCI

DSL Network Settings

Configuration – Network > Interfaces > DSL> DSL Network Settings

This DSL PVC is using PPP 1
The default interface for DSL is PPP 1

Description
Enter a description for the DSL if required

Username
Enter ADSL Username

Password
Enter the password for the DSL account

Confirm password
Enter the password for the DSL account

Enable NAT on this interface
This parameter is used to select whether IP Network Address Translation (NAT) or Network Address and Port Translation (NAPT) are used at the Ethernet interface. When the parameter is set to disabled, no NAT will take place. When this parameter is enabled, extra options described below will be displayed.

NAT and NAPT can have many uses but they are generally used to allow a number of private IP hosts (PCs for example) to connect to the Internet through a single shared public IP address. This has two main advantages, it saves on IP address space (the ISP only need assign you one IP address), and it isolates the private IP hosts from the Internet, effectively providing a simple firewall because unsolicited traffic from the Internet cannot be routed directly to the private IP hosts.

To use NAT or NAPT correctly in the example of connecting private hosts to the Internet, NAT or NAPT should be enabled on the router's WAN side interface and should be disabled on the router's LAN side interface.

IP address
Enable standard Network Address Translation (NAT).

When a private IP host sends a UDP or TCP packet to an Internet IP address, the router will change the source address of the packet from the private host IP to the router's public IP address before forwarding the packet onto the Internet host. Additionally it will create an entry in a "NAT table" containing the private IP source address, the private IP port number, the public IP destination address and the destination port number. Conversely, when the router receives a reply packet back from the public host, it checks the source IP, source port number and destination port number in the NAT table to determine which private host to forward the packet to. Before it forwards the packet back to the private host, it changes the destination IP address of the packet from its public IP address to the IP address of the private host.

IP address and Port
Enable Network Address and Port Translation (NAPT).

This mode behaves like NAT but in addition to changing the source IP of the packet from the private host it can also change the source port number. This is required if more than one private host attempts to connect using the same local port number to the same Internet host on the same remote port number. If such a scenario were to occur with NAT the router would be unable to determine which private host to route the returning packets to and the connection would fail.

NAT Source IP address
If specified, and NAT mode has been set to "NAT" or "NATP" for this interface, then the source address of packets being sent out this interface is changed to this address, rather than the interface address.

Enable IPsec on this interface
The IPSec parameter is used to enable or disable IPSec processing on this interface. If this box is ticked, packets sent or received on this interface must pass through the IPSec code before being transmitted. IPSec may drop the packet, pass it unchanged, or encrypt and encapsulate within an IPSec packet.

Keep Security Associations (SAs) when this Mobile interface is disconnected
This checkbox will configure the router to keep any existing IKE and IPsec associations should the link drop. This is usually applied on head-end routers with fixed IP addresses.

Use interface X, Y for the source IP address of IPsec packets
By default, the source IP address for an IPSec Eroute will be the IP address of the interface on which IPSec was enabled. By setting this parameter to either a PPP or Ethernet interface, the source IP address used by IPSec will match that of the Ethernet or PPP interface specified.

Enable the firewall on this interface
The Firewall parameter is used to turn Firewall script processing "On" or "Off" for this interface.

> **Note:**
> If the firewall is enabled on an interface and with the absence of any firewall rules, the default action is to block ALL traffic.
> To configure the firewall see Configuration – Security > Firewall

Limit the data transmitted over this interface

On W-WAN networks (where charging is based on the amount of data transferred as opposed to time spent on-line), this parameter may be used to specify a data limit after which the unit will create an entry in the event log to indicate that this amount of data has been transferred. For example, if your monthly tariff includes up to 5Mb of data before you are charged an "excess", you might set the Data limit warning level to 4000. This would cause the unit to place a warning entry in the event log once you had transferred 4Mb. This event could be used to trigger an email alert message, SNMP trap or SMS alert message.

Issue a warning event after

Enter the maximum data to be transmitted before a warning entry is generated in the eventlog. You have the option to select Kbytes, Mbytes or GBytes via the drop-down box.

Stop data from being transmitted after

This parameter is used to set the maximum amount of data that may be transferred before the unit will "lock" the interface and prevent further transfer. As with the *Issue a warning event after* parameter it is used on networks where the tariff is based on the amount of data transferred to help prevent excess charges being incurred. You have the option to select Kbytes, Mbytes or GBytes via the drop-down box.

Reset the data limit on the x day of the month

If you wish to automatically unlock a locked interface at the start of a new billing period, this parameter should be set to the appropriate day of the month (from 1 to 28). When this date is reached the unit will unlock the interface and data transfer may resume. If the parameter is set to 0, automatic unlocking will not occur and manual unlocking will be necessary (by clicking on the **Clear Total Data Transferred** button on the appropriate ***Diagnostics - Statistics > PPP > PPP n*** page. This parameter will also reset the statistics for the **Data limit warning level (kb)**.

The factory default does not include any DSL settings and so when the router is first installed, the following text will appear.
"This DSL PVC is not assigned to any PPP interface
Click here to jump to the PPP Mapping page"
When clicked, this link will redirect the browser to the ***Configuration – Network > interfaces > Advanced > PPP Mappings*** page.
From this page, select the desired PPP instance. The PPP instance.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	1	description	Free text	Description
ppp	1	username	Free text	Username
ppp	1	password	Free text	Password
ppp	1	do_nat 1	ON	Enable NAT on this interface (IP Address)
ppp	1	do_nat 2	ON	Enable NAT on this interface (IP Address and port)
ppp	1	natip	IP Address	NAT Source IP Address
ppp	1	ipsec	ON/OFF	Enable IPSec on this interface
ppp	1	firewall	ON/OFF	Enable the firewall on this

Entity	Instance	Parameter	Values	Equivalent Web Parameter
				interface
ppp	1	dlwarnkb	Kbytes/Mbytes/GBytes	Issue a warning event after
ppp	1	dlstopkb	Kbytes/Mbytes/GBytes	Stop data from being transmitted after x Bytes data
ppp	1	dlrstday	1-28	Reset the data limit on the nth day of the month

PVC Traffic Shaping

Configuration – Network > Interfaces > DSL> PVC Traffic Shaping

Service category

Each ATM PVC may now be configured with a service category:
UBR (unspecified bit rate, the default)
VBR-nrt (variable bit rate, non-real-time)
VBR-rt (variable bit rate, real-time)
CBR (constant bit rate)

Additional traffic parameters may be specified:
PCR (peak cell rate in cells/sec)
SCR (sustained cell rate in cells/sec)
MBS (maximum burst size in cells)

The four service categories are characterised by the various traffic parameters as follows:
UBR: PCR, which may be zero for no limit
VBR-nrt: PCR, SCR, MBS
VBR-rt: PCR, SCR, MBS
CBR: PCR

Peak cell rate (cells/sec)

The maximum allowable rate at which cells can be transported along a connection in the ATM network. The PCR is the determining factor in how often cells are sent in relation to time in an effort to minimize jitter. PCR generally is coupled with the CDVT (Cell Delay Variation Tolerance), which indicates how much jitter is allowable

Sustained cell rate (cells/sec)

A calculation of the average allowable, long-term cell transfer rate on a specific connection.

Maximum burst size (cells)
The maximum allowable burst size of cells that can be transmitted contiguously on a particular connection.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
apvc	0	servcat	UBR,VBR-ntr,VBR-rt,CBR	Service category
apvc	0	pcr	n	Peak cell rate (cells/sec)

Entity	Instance	Parameter	Values	Equivalent Web Parameter
apvc	0	scr	n	Sustained cell rate (cells/sec)
apvc	0	mbs	n	Maximum burst size (cells)

Advanced

Configuration – Network > Interfaces > DSL> Advanced

Operational mode
This parameter is used to specify the connection mode for the DSL link. The following options are available (default is Multi mode).

Values	Equivalent Web Parameter
Multi-mode	For Annex A models (i.e. PSTN / POTS) this option provides automatic selection between G.dmt, G.lite and ANSI (in the order listed). For Annex B models (i.e. ISDN) this option provides automatic selection between G.dmt (in the order listed)
ANSI	Annex A only - attempt to connect in ANSI T1.413 mode
G.dmt	Attempt to connect in ITU G.992.1 G.dmt mode
G.lite	Annex A only - attempt to connect in ITU G.992.2 G.lite mode
ADSL2	Connect using ADSL2
ADSL2+	Connect using ADSL2+

Load DSL firmware from flash file 'dspfw.bin' (if present)
This checkbox enables the use of alternative ADSL driver firmware and should only be enabled on the advice of the technical support team. This option also requires that an additional file be loaded onto the router.

Enable watchdog
This checkbox should only be enabled on the advice of the technical support team.

Manage this PVC using ATM OAM cells
Using Alarm indication signal (AIS) cells downstream and Remote defect indication (RDI) cells upstream, the router can detect faults between the connecting points of the VP/VC and suspend transfer of ATM cells until the VC fault condition is cleared.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
adsl	0	oper_mode	Multi,ANSI,G.dmt, G.lite,ADSL2, ADSL2+	Operational mode
adsl	0	usefwfile	ON/OFF	Load DSL firmware from flash file
adsl	0	watchdog	ON/OFF	Enable watchdog

Entity	Instance	Parameter	Values	Equivalent Web Parameter
apvc	0	oammanage	ON/OFF	Manage this PVC using ATM OAM cells

Additional CLI commands

The following command is not available from the web interface:

adsl 0 debug {0|1}

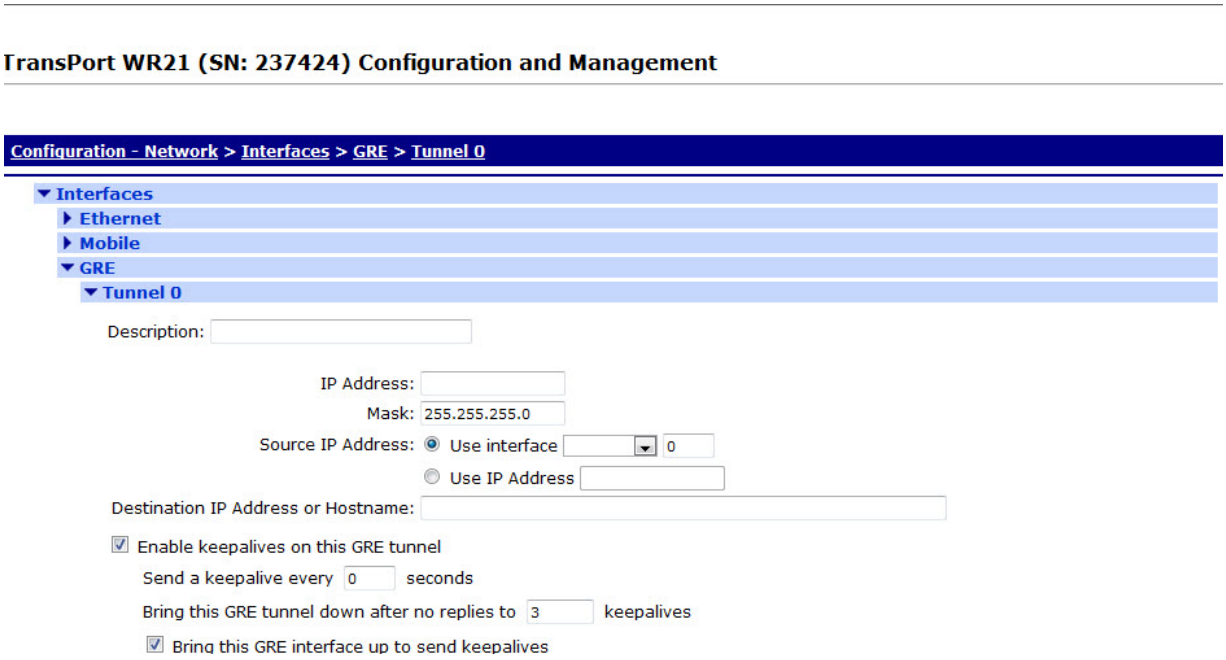
Where 0 is off and 1 causes debugging information to be sent to the CLI.

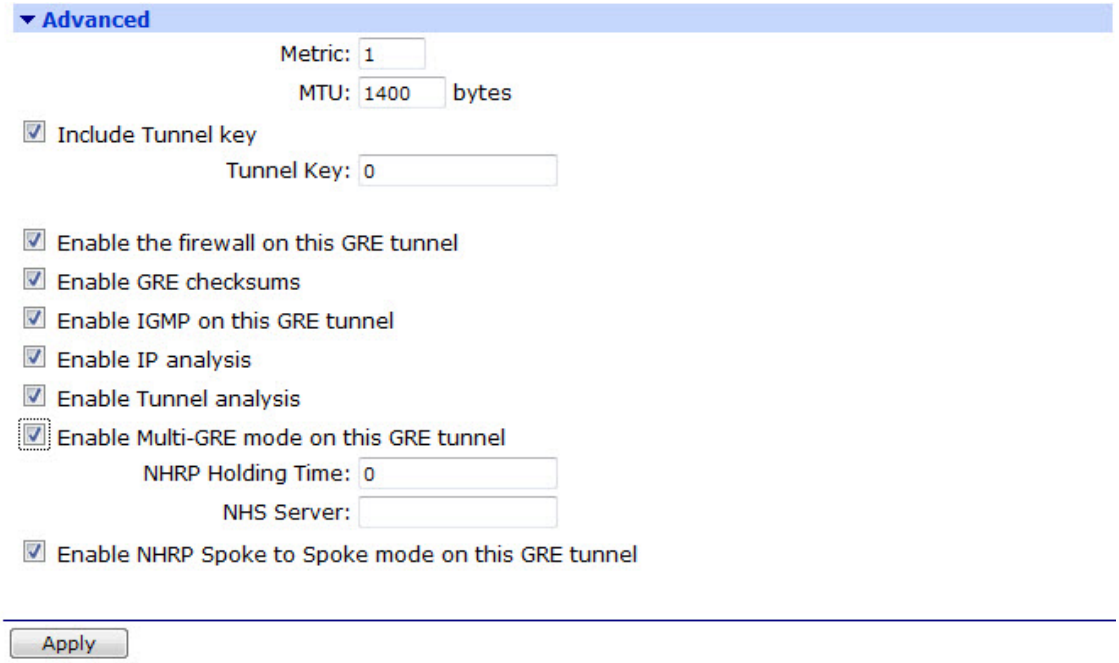
GRE

Configuration – Network > Interfaces > GRE

Generic Routing Encapsulation (GRE) is a means of transporting IP packets from one device to another through an unencrypted point-to-point IP tunnel. Multiple tunnels may be configured to multiple devices. Below the GRE Interfaces (***Configuration - Network > Interfaces > GRE***) sub menu you will find the individual tunnel configuration. When configured, a GRE tunnel will be created between 2 devices.

Tunnel n


TransPort WR21 (SN: 237424) Configuration and Management
Configuration - Network > Interfaces > GRE > Tunnel 0
Interfaces
Ethernet
Mobile
GRE
Tunnel 0
Description:
IP Address:
Mask: 255.255.255.0
Source IP Address: Use interface 0
Use IP Address
Destination IP Address or Hostname:
Enable keepalives on this GRE tunnel
Send a keepalive every 0 seconds
Bring this GRE tunnel down after no replies to 3 keepalives
Bring this GRE interface up to send keepalives



Configuration – Network > Interfaces > GRE> Tunnel

Description:
This parameter allows you to enter a name for this GRE instance, to make it easier to identify it.

IP address:
This is the IP address of the virtual interface that will be used by the tunnel. This parameter is used in conjunction with the mask parameter below. This parameter MUST be entered for the tunnel to work.

Mask:
Used with the IP address parameter to clarify the subnet in use on the virtual interface. This would normally be a 30 bit mask as this is a point-to-point link (255.255.255.252).

Source IP Address:
The two sub options here will allow you to specify a source address either from a specified interface or by manually assigning an address. If you do not select either option the default address for the route the packet leaves the router through will be used (please note that if the interface through which the GRE packets exit does not have natting turned on then the default router address will be used – by default this will be the Ethernet 0 address).

Use Interface:
These 2 parameters allow you to select the GRE tunnel source interface, so the tunnel end point can be a physical interface rather than a virtual IP address. This is for using GRE without IPSec. These parameters should not be used if the source address is used in the parameter below. Select from the drop down boxes the available interface type and number.

Use IP Address:
A virtual host IP address for the local end of the tunnel, configured for routing purposes. This IP address has no other use and needs no mask as it is a host address. e.g. 1.1.1.1.

This option is normally used in conjunction with IPSec. This parameter should not be used if the interface is selected as the source using the “Use Interface” options above.

Destination IP Address or Hostname:
This is the FQDN or IP address of the remote end of the tunnel. This could also be the virtual host IP address for the remote end of the tunnel, configured for routing purposes. e.g. 2.2.2.2

Enable keepalives on this GRE tunnel

Selecting this checkbox will display the GRE keepalive parameters. Keepalives are needed so allow the router to determine whether the tunnel interface is receiving traffic correctly or not. If keepalives fail, the tunnel will be marked as down.

Send a keepalive every s seconds

When configured to a non-zero value, keepalive packets will be sent to the remote end of the tunnel and the response is monitored to detect if the tunnel is up or down. If the tunnel is detected as down, the routing table metric will be altered. Value is configured in seconds. If this value is set to zero then keepalives will not be used.

Bring this GRE tunnel down after no replies to n keepalives

This parameter specifies the consecutive number of keepalive packets that need to fail before the tunnel is detected as being down.

Bring this GRE interface up to send keepalives
This specifies whether or not the GRE keepalive packets will activate the tunnel. If set to YES and the tunnel drops the GRE keepalive packet will try to raise the tunnel again. If set to NO and the tunnel has been marked as down due to the GRE keepalives not being received, the router will only raise the tunnel if a packet (other than a GRE keepalive) needs to be routed.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
tun	n	descr	Free text field	Description
tun	n	IPaddr	Valid IP address	IP Address
tun	n	mask	Valid Subnet Mask	Mask
tun	n	source_ent	blank,ETH,PPP	Use interface x,y for the source IP address of GRE packets x = Interface type
tun	n	source_add	0 - 255	Use interface x,y for the source IP address of GRE packets y = interface number
tun	n	source	Valid IP address	Source IP address to use for GRE packets
tun	n	dest	Valid IP address	Destination IP address to use for GRE packets
tun	n	Kadelay	Seconds	Send a keepalive every s seconds
tun	n	karetries	Number	Bring this GRE tunnel down after no replies to n keepalives

Entity	Instance	Parameter	Values	Equivalent Web Parameter
tun	n	kaactrq	On,off	Bring this GRE interface up to send keepalives

Advanced

Configuration – Network > Interfaces > GRE> Tunnel> Advanced

Metric:
This parameter specifies the connected metric of an interface. The default metric of a connected interface is 1. By allowing the interface to have a higher value (lower priority), static routes can take preference to interfaces. For normal operation, leave this value unchanged.

MTU:
Maximum Transmission Unit. The value entered here will be the greatest amount of data that can be transferred in one physical packet. Default value is 1400

Include Tunnel Key

When this parameter is enabled, a non-zero tunnel key value in the configuration file will be copied over into the key parameter.

Tunnel Key:
Normally used with multi GRE (mGRE), the tunnel key adds an extra field to the GRE header where a key number can be applied. When used, incoming GRE packets must have a matching tunnel key number to be accepted by this tunnel. When the Tunnel key parameter is used the IP address parameter is not required.

Enable the firewall on this GRE tunnel:
The Firewall parameter is used to turn Firewall script processing “On” or “Off” for this interface. If using the firewall for problem detection on a tunnel interface, the interface to put OOS will need to be specified, e.g.:

pass out break end on tun n from any to 100.100.100.29 port=4000 flags S!A inspect-state oos ppp n 5

Enable GRE checksums:
This parameter selects whether to add GRE checksums to GRE packets when the unit is terminating a GRE tunnel. “Off” disables checksums, “On” enables checksums.

Enable IGMP on this GRE tunnel:
This IGMP parameter is used to enable or disable the transmission and reception of IGMP packets on this interface. IGMP is used to advertise members of multicast groups. If IGMP is enabled, and a member of a multicast group is discovered on this interface, multicast packets for this group received on other interfaces will be sent out this interface.

Enable IP analysis:
When set to ON, the un-encapsulated IP traffic will be captured into the analyser trace.

Enable Tunnel analysis:
When set to ON, the GRE encapsulated packets and keepalives will be captured to the analyser trace.

Enable multi-GRE mode on this GRE tunnel
When set to ON, the the multi-GRE mode is enabled on the GRE tunnel and uses NHRP to determine the direct tunnel addresses

NHRP holding time
This is the NHRP hold time in seconds. This is used in the NHRP registration process and advices the server how long our registration information should be held for. The NHRP client will repeatedly register whilst the tunnel is up so that a small time can be considered.

NHS Server
This defines the NHS servers tunnel address which is needed in the NHRP registration process

Enable NHRP spoke to spoke mode on this GRE tunnel
When set to ON, the NHRP spoke to spoke mode is enabled on the GRE tunnel.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
tun	n	metric	Numeric Metric value	Metric for the route associated with this interface
tun	n	MTU	MTU value	Maximum transmission unit size
tun	n	key	On/ Off	Include Tunnel Key
tun	n	tunkey	Key number	Tunnel Key
tun	n	Firewall	on,off	Turn firewall on or off
tun	n	csum	on,off	Enable GRE checksums
tun	n	igmp	On, off	Enable IGMP packets
tun	n	ipanon	On, off	Enable IP analysis
tun	n	tunanon	On, off	Enable tunnel analysis
tun	n	mgre	On, Off	Enable multi-GRE mode on this GRE tunnel
tun	n	nhrp_holdtime	seconds	NHRP holding time
tun	n	nhs	server name	NHS Server
tun	n	nhrp_auth	string	
tun	n	spoke2spoke	On, Off	Enable NHRP spoke to spoke mode on this GRE tunnel

RIP Routing Parameters – CLI only

Please note that under the CLI commands for GRE Tunnels you will find parameters specifically relating to RIP. Please see the **Configuration – Network > IP Routing / Forwarding > RIP > Interfaces > Ethernet / PPP / GRE** section on RIP routing for configuration of these sub parameters.

ISDN

Configuration - Network > Interfaces > ISDN

The ***Configuration - Network > Interfaces > ISDN*** page has the following options:

- ISDN Answering
- ISDN Dialling

- LAPD

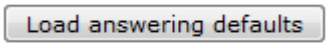
ISDN Answering

Configuration - Network > Interfaces > ISDN> ISDN Answering

This page allows you to configure the ISDN interface to receive incoming calls.

Button:- Load answering defaults

Clicking this button resets the default answering PPP interface (PPP 0) to the factory answering defaults.



Description:
This parameter allows you to enter a name for this PPP instance, to make it easier to identify it.

Only accept calls from calling numbers

ending with
This parameter is used to restrict the range of numbers from which ISDN will answer incoming calls, i.e. the ISDN interface will only answer a call if the trailing digits of the calling number match what is specified by this parameter. For example, if this parameter was set to 3, incoming calls from 1234563 would be answered but calls from 1234567 would not.

with ISDN MSN ending with
If answering is disabled this parameter is not used.
This parameter provides the filter for the ISDN Multiple Subscriber Numbering facility. It is blank by default but when set to an appropriate value on an answering interface, it will cause the unit to answer incoming calls to only telephone numbers where the trailing digits match the value selected. For example, setting this parameter to 123 will prevent the unit from answering any calls to numbers that do not end in 123.

with ISDN sub-address ending with
If answering is disabled this parameter is not used.
This parameter provides the filter for the ISDN sub-address facility. It is blank by default but when set to an appropriate value on an ISDN answering interface, it will cause the unit to answer incoming calls only to ISDN numbers where the trailing digits match the Sub-address value. For example, setting the this parameter to 123 will prevent the unit from answering any calls to numbers that do not end in 123.

Use the following local IP configuration

Local IP Address:
This is the IP address of the unit's ISDN answering interface. Set this field to the desired local IP address.

Attempt to assign the following IP configuration to remote devices
Set this parameter if it is required that the remote system have an address supplied. An attempt to negotiate an IP address from the IP address pool will be made. Generally, this parameter is enabled for incoming connections.
This checkbox opens to show the following parameters:-

Assign remote IP addresses from a.b.c.d to a.b.c.d

This is the range of IP addresses supplied to incoming callers. This parameter may require alteration if the default value “10.10.10.0” to “10.10.10.4” does not suit the remote network configuration.

Mask:
This specifies the IP netmask for the Remote network. This can be used to create a dynamic route to the remote network whenever the ISDN interface is active.

Primary DNS server:
The answering ISDN interface would normally supply its own PPP IP address to the peer for DNS requests. This allows you to specify an alternative DNS IP address.

Secondary DNS server:
This parameter can supply a secondary DNS server IP address to the peer for DNS requests if required.

Enable NAT on this interface
This parameter is used to enable or disable IP Network Address Translation (NAT) on the answering ISDN interface.
This checkbox opens to show the following options:-

IP Address:
Enable standard Network Address Translation (NAT).

IP address and Port:
Enable Network Address and Port Translation (NAPT).

Enable IPsec on this interface
This parameter is used to enable or disable IPSec processing on the ISDN interface. If enabled, packets sent or received on this interface must pass through the IPSec code before being transmitted. IPSec may drop the packet, pass it unchanged, or encrypt and encapsulate within an IPSec packet.
This checkbox opens to show the following parameters:-

Keep Security Associations (SAs) when this ISDN interface is disconnected
This checkbox will configure the router to keep any existing IKE and IPsec associations should the link drop. This is usually applied on head-end routers with fixed IP addresses.

Use interface X, Y for the source IP address of IPsec packets
By default, the source IP address for an IPSec Eroute will be the IP address of the interface on which IPSec was enabled. By setting this parameter to either a PPP or Ethernet interface, the source IP address used by IPSec will match that of the Ethernet or PPP interface specified.

Enable the firewall on this interface
The Firewall parameter is used to enable or disable the Firewall script processing for the mobile interface.

Note:
If the firewall is enabled on an interface and with the absence of any firewall rules, the default action is to block ALL traffic.
To configure the firewall see Configuration > Security > Firewall

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	0	name	Free text field	Description:

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	0	cingnb	number	ending with
ppp	0	msn	number	with ISDN MSN ending with
ppp	0	sub	number	with ISDN sub-address ending with
ppp	0	ipaddr	IP address	Local IP Address:
ppp	0	mask	Network mask	Mask:
ppp	0	ipmin	IP address	Assign remote IP addresses from a.b.c.d to a.b.c.d
ppp	0	iprange	1 - 255	Assign remote IP addresses from a.b.c.d to a.b.c.d
ppp	0	dnsserver	IP address	Primary DNS server:
ppp	0	secdns	IP address	Secondary DNS server:
ppp	0	do_nat	1	Enable NAT on this interface IP Address:
ppp	0	do_nat	2	Enable NAT on this interface IP address and Port:
ppp	0	ipsec	1	Enable IPsec on this interface
ppp	0	ipsec	2	Keep Security Associations (SAs) when this ISDN interface is disconnected
ppp	0	ipsecent	Default,Ethernet, PPP	Use interface X, Y for the source IP address of IPsec packets
ppp	0	ipsecadd	number	Use interface X, Y for the source IP address of IPsec packets
ppp	0	firewall	on/off	Enable the firewall on this interface

Advanced

Configuration - Network > Interfaces > ISDN> ISDN Answering> Advanced

These are the advanced settings for the ISDN interface.

Metric:
This parameter specifies the connected metric of the mobile interface. The default metric of a connected interface is 1. By allowing the interface to have a higher value (lower priority), static routes can take preference to interfaces. For normal operation, leave this value unchanged.

Enable "Always On" mode of this interface

On
This parameter is used to configure the PPP instance so that in the event that it is disconnected the unit will try to reconnect again after approximately 10 seconds or dictated by the ***Configuration - Network > IP Routing/Forwarding > IP Routing >***

When an "Always On" route becomes "In Service", wait n seconds before using it parameter.

On and return to service immediately
As above “On” but the unit will try and connect immediately and without delay.

Put this interface "Out of Service" when an always-on connection attempt fails
Usually, always-on interfaces will not go out of service unless they have connected at least once. When this option is turned “On”, the interface will go out of service even if the first connection attempt fails.

Attempt to re-connect after n seconds
This parameter specifies the length of time in seconds that the unit will wait after an “always-on” ISDN connection has been terminated before trying to re-establish the link.

If an inhibited PPP interface is connected, attempt to re-connect after n seconds
The value of this parameter takes precedence over ***Configuration - Network > Interfaces > ISDN > ISDN Answering > Advanced > Wait n seconds after power-up before activating this interface*** when some other PPP that is usually inhibited by this one is connected. This parameter would typically be used to reduce the connection retry rate when a lower priority PPP is connected.

Wait n seconds after power-up before activating this interface
If this parameter is not set to “0”, this is the initial delay after power up before the PPP will activate. After that, the usual always-on activation timers apply.

Control when this interface can connect using Time band n

This parameter specifies the Time Band number to use for this ISDN instance (see ***Configuration - Network > Timebands***).

Keep this interface up for at least n seconds
If this parameter is set to a non-zero value, then ISDN will not close the connection for the specified period, even if the link is inactive.

Close this interface

After n seconds
This parameter specifies the maximum time that this ISDN Interface may remain connected during any one session. After this time, the ISDN link is deactivated.

If it has been up for n minutes in a day
This parameter specifies the maximum time that this ISDN interface may remain connected during any one day. After this time, the ISDN link is deactivated.

If the link has been idle for n seconds
The ISDN interface will close the connection if the link is inactive for the length of time specified by this parameter.

Alternative idle timer for static routes n seconds
This parameter may be used to specify an alternative Inactivity timeout for use in conjunction with the Use 2nd inactivity timeout when this route becomes available parameter on the Configuration - Routing > Routing > Static Route n pages. This timeout will only be used until the PPP next deactivates. After that, the normal timeout value is used.

If the link has been idle for s seconds
The router will deactivate this interface after the time specified in this text box if it detects that the link has not passed any traffic for that period.

Alternative idle timer for static routes s seconds
The value in this text box specifies an alternative inactivity timeout for use in conjunction with the "Make PPP n interface use the alternative idle timeout when this route becomes available" parameter on the ***Configuration – Network > IP Routing/Forwarding > Static Routes > Routes n > Advanced*** web page. This timeout will only be used until the PPP instance next deactivates. After that the normal timeout value is used.

If the link has not received any packets for s seconds
The value in this text box specifies the amount of time that the router will wait without receiving any PPP packets before disconnecting. The timer is reset with each received PPP packet.

If the negotiation is not complete in s seconds
The value in this textbox specifies the maximum time (in seconds) allowed for the PPP negotiation to complete. If negotiations have not completed within this period, the interface is deactivated.

Generate an event after this interface has been up for m minutes
The value in this text box specifies the number of minutes (if any) after which the router should create an event in the event log that states that the interface has been active for this period.

Limit the data transmitted over this interface
When checked, this checkbox reveals the following parameters that control what data volume restrictions (if any) should be applied to this interface:

Issue a warning event after n units
The value in this text box is the amount of traffic which will cause a warning event to be generated in the event log stating that the specified amount of data has been transferred. The units are specified by a drop-down list, having the following options; KBytes, MBytes, GBytes. For example, if the monthly tariff includes up to 5MB of data before excess usage charges are levied, it would be useful to set this threshold to 4MB. This would cause the router to create a warning entry in the event log once 4MB of data had been transferred. This event could then be used to trigger an email alert, SNMP trap or SMS alert message.

Stop data from being transmitted after n units
The value in this text box specifies the total amount of data that may be transmitted by this PPP instance before the link is blocked for further traffic, and the value in the drop-down list specifies the units which are; KBytes, MBytes, GBytes.

Reset the data limit on the n day of the month
The value in this text box defined the day of the month on which the data limit is reset to zero.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	metric	0 - 255	Metric
ppp	n	aodion	0 – 2 0 = disabled 1 = enabled 2 = On and return to service immediately	Enable "Always On" mode of this interface, On, On and return to service immediately
ppp	n	immoos	ON, OFF	Put this interface "Out of

Entity	Instance	Parameter	Values	Equivalent Web Parameter
				Service" when an always-on connection attempt fails
ppp	n	aodi_dly	0 – 2147483647	Attempt to reconnect after s seconds
ppp	n	aodi_dly2	0 – 2147483647	If an inhibited PPP interface is connected, attempt to re-connect after s seconds
ppp	n	pwr_dly	0 – 2147483647	Wait s seconds after power-up before activating this interface
ppp	n	tband	0 - 4	Control when this interface can connect using Time Band n
ppp	n	minup	0 – 2147483647	Keep this interface up for at least s seconds
ppp	n	maxup	0 – 2147483647	Close this interface after s seconds
ppp	n	maxuptime	0 – 2147483647	if it has been up for m minutes in a day
ppp	n	timeout	0 – 2147483648	if the link has been idle for s seconds
ppp	n	timeout2	0 – 2147483648	Alternative idle timer for static routes s seconds
ppp	n	rxtimeout	0 – 2147483648	if the link has not received any packets for s seconds
ppp	n	maxneg	0 – 2147483648	if the negotiation is not complete in s seconds
ppp	n	uplogmins	0 – 2147483647	Generate an event after this interface has been up for m mins
ppp	n	dlwarnkb	0 – 2147483647	Issue a warning after n units
ppp	n	dlstopkb	0 – 2147483647	Stop data from being transmitted after n units
ppp	n	dlrstday	0 – 255	Reset the data limit on the n day of the month

ISDN Dialling

Configuration - Network > Interfaces > ISDN> ISDN Dialing

This section of the web interface appears when the router is fitted with an optional internal ISDN MODEM card. When first powered up, navigating to the ***Configuration – Network > Interfaces > ISDN*** page will show a message indicating that the MODEM card does not have a PPP instance associated with it. Follow the link on the page and select an unassigned PPP interface to the MODEM. When the browser is refreshed and the ***Configuration – Network > Interfaces > ISDN*** page redisplayed, it should show the parameters described below, along with a message at the top of the page indicating which PPP instance has been selected.

This ISDN interface is using PPP n
This message simply states which PPP instance has been assigned to the interface.

Description
The value in this text box is a memorable name for the interface. This may be useful when referring to the interface, rather than having to remember the name and the function of the interface.

Dial out using numbers
These four text boxes contain the telephone numbers that should be used, in sequence, to make an outgoing connection.

Prefix n to the dial out number
The value in this text box specifies the dialling prefix to use, if needed. This may be necessary when using a PABX.

Username
The text string text box is the username that should be used when using the PPP instance to connect to the remote peer. This will normally be provided by an ISP for use with a dial-in Internet access service.

Password
This text box contains the password to use for authenticating the remote peer and is used in conjunction with the above username.

Confirm password
Type the password into this text box to enable the router to confirm that the password has been entered identically in both boxes.

Allow the remote device to assign a local IP address to this router

When this radio button is selected, the remote peer will assign this PPP interface an IP address.

Try to negotiate a.b.c.d as the local IP address for this router

If it would be useful, but not essential, to have a predefined IP address for the interface, the second radio button should be selected and the desired IP address entered into the text box to the right.

Use a.b.c.d as the local IP address for this router

If it is essential that the PPP interface has a specific IP address, this radio button should be selected and the IP address entered into the text box.

Use the following DNS servers if not negotiated

Primary DNS server
The value in this text box is the IP address of the primary DNS server to use if a DNS server is not assigned as part of the PPP negotiation and connection process. It is fairly

common practice for the DNS server to be assigned automatically by the ISP when making a connection.

Secondary DNS server
The value in this text box specifies the IP address of the secondary DNS server to use if one is not automatically assigned by the remote peer.

Attempt to assign the following IP configuration to remote devices
When checked, this check box will reveal the following four configuration parameters which control how the PPP instance assigns an IP address to a connecting remote peer. The primary and secondary DNS server addresses will also be sent to the remote peer

Assign remote IP addresses from a.b.c.d to a.b.c.d
The IP addresses in these text boxes define the pool of IP addresses to assign to remote peers during the IP protocol configuration phase of the PPP negotiation process.

Primary DNS server
The value in this text box is the IP address of the primary DNS server that the remote peer should use when making DNS requests over the link.

Secondary DNS server
The value in this text box is the IP address of the secondary DNS server that the remote peer should use when making DNS requests, should the primary server be unavailable.

Allow the PPP interface to answer incoming calls
When checked, this checkbox will cause the PPP instance to answer an incoming call.

Only allow calling numbers ending with n
When set to answer calls, the value in this textbox provides a filter for ISDN sub-addresses. This value is blank by default but when the PPP instance is set to answer calls, only numbers having trailing digits that match the sub-address value in this test will be answered. So for example, if this value is set to “123”, only calls from numbers with trailing digits that match this value will be answered. For example 01942 605123

Enable NAT on this interface
When checked, this checkbox will enable Network Address Translation to operate on this interface. This is the same as for other PPP interfaces.

IP address / IP address and Port
These radio buttons select whether IP address translation only should be applied or whether port number translation should also be applied to IP packets.

Enable IPsec on this interface
When checked, this checkbox will cause the router to encrypt traffic on this interface using the IPsec protocol. The following two additional configuration parameters are revealed when this box is checked.

Keep Security Associations (SAs) when this ISDN interface is disconnected
When checked, this checkbox causes the router to maintain (i.e. not flush) the SA when the interface becomes disconnected. The normal behaviour is to remove the SAs when the interface becomes disconnected.

Use interface x,y for the source IP address of IPsec packets
If it is required to use another interface (i.e. not the interface currently being configured) as the source address for IPsec packets, this may be achieved by selecting the desired interface from the drop-down list and typing the desired interface instance number into the adjacent text box.

Enable the firewall on this interface

When checked, this checkbox applies the firewall rules to traffic using this interface.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	name	Up to 25 characters	Description
ppp	n	phonenum	up to 25 digits	Dial out using numbers
ppp	n	ph2	“	“
ppp	n	ph3	“	“
ppp	n	ph4	“	“
ppp	n	prefix	0 – 9999999999	Prefix n to the dial out number
ppp	n	username	Up to 60 characters	Username
ppp	n	password	Up to 40 characters	Password
ppp	n	IPaddr	0.0.0.0	Allow the remote device to assign a local IP address to this router
ppp	n	IPaddr	Valid IP address a.b.c.d	Try to negotiate a.b.c.d as the local IP address for this router (in conjunction with l_addr)
ppp	n	l_addr	OFF,ON When ON, allows negotiation when OFF force use of specified IP address	Use a.b.c.d as the local IP address of this router
ppp	n	DNSserver	Valid IP address a.b.c.d	Use the following DNS servers if not negotiated Primary DNS server a.b.c.d
ppp	n	secDNS	Valid IP address a.b.c.d	Use the following DNS servers if not negotiated Secondary DNS server a.b.c.d
ppp	n	IPmin	Valid IP address a.b.c.d	Assign remote IP addresses from a.b.c.d to a.b.c.d
ppp	n	IPrange	0 - 255	Assign remote IP addresses from a.b.c.d to a.b.c.d
ppp	n	transDNS	Valid IP address a.b.c.d	Primary DNS server a.b.c.d
ppp	n	sectransDNS	Valid IP address a.b.c.d	Secondary DNS server a.b.c.d
ppp	n	ans	OFF,ON	Allow this PPP interface to answer incoming calls

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	cingnb	up to 25 digits	Only allow calling numbers ending with n
ppp	n	do_nat	0,1,2 0 = Disabled 1 = IP address 2 = IP address and port	Enable NAT on this interface IP address/IP address and Port
ppp	n	nat_ip	Valid IP address a.b.c.d	NAT Source IP address a.b.c.d
ppp	n	ipsec	0 = Disabled 1 = Enabled 2 = Enabled and Keep SAs	Enable IPsec on this interface/ Keep Security Associations when this ISDN interface is disconnected
ppp	n	firewall	OFF,ON	Enable the firewall on this interface

Advanced

Configuration - Network > Interfaces > ISDN> ISDN Dialling> Advanced

Metric
The value in this text box specifies the route metric that should be applied to this interface. (see ***Configuration – Network > Interfaces > Advanced > PPP n*** for more detail.)

Enable "Always On" mode of this interface
When checked, this checkbox causes the following two options to appear:

On / On and return to service immediately
These two radio buttons select whether the "always-on" functionality should simply be enabled or whether the additional facility to return the interface to the "In Service" state should be applied.

Put this interface "Out of Service" when an always-on connection attempt fails
Normally, always-on interfaces will not go out of service unless they have connected at least once. When checked, this checkbox causes the router to put the interface out of service even if the first connection attempt fails.

Attempt to re-connect after s seconds
The parameter in this text box specifies the length of time in seconds that the router should wait after an "always-on" PPP connection has been terminated before trying to re-establish the link.

If an inhibited PPP interface is connected, attempt to re-connect after s seconds
The value in this text box takes precedence over the previous parameter when another PPP instance that is usually inhibited by this one is connected. This parameter would typically be used to reduce the connection retry rate when a lower priority PPP instance is connected.

Wait s seconds after power-up before activating this interface
The value in this text box is the initial delay that the router will apply before activating the PPP instance after power-up. After the initial power-up delay the normal always-on activation timers apply. If set to zero, no delay will be applied.

Control when this interface can connect using Time band n
These two controls, the check box and drop-down list determine whether the Time Band function should be applied to this interface. Checking the checkbox enables the functionality and the desired time band instance is selected from the drop-down list. Time Band functionality is explained in the ***Configuration – Network > Interfaces > Timebands*** section of this manual.

Keep this interface up for at least s seconds
The value in this textbox specifies the minimum period that the PPP interface should remain available. This means that even if the link becomes inactive before this period expires, the connection will remain open.

Close this interface

After s seconds
The value in this text box specifies the maximum time that the link will remain active in any one session. After this time, the link will be deactivated.

If it has been up for m minutes in a day
The router will deactivate the PPP instance after it has been active for the value specified in this text box.

If the link has been idle for s seconds
The router will deactivate this interface after the time specified in this text box if it detects that the link has not passed any traffic for that period.

Alternative idle timer for static routes s seconds
The value in this text box specifies an alternative inactivity timeout for use in conjunction with the "Make PPP n interface use the alternative idle timeout when this route becomes available" parameter on the ***Configuration – Network > IP Routing/Forwarding > Static Routes > Routes n > Advanced*** web page. This timeout will only be used until the PPP instance next deactivates. After that the normal timeout value is used.

If the link has not received any packets for s seconds
The value in this text box specifies the amount of time that the router will wait without receiving any PPP packets before disconnecting. The timer is reset with each received PPP packet.

If the negotiation is not complete in s seconds
The value in this textbox specifies the maximum time (in seconds) allowed for the PPP negotiation to complete. If negotiations have not completed within this period, the interface is deactivated.

Generate an event after this interface has been up for m minutes
The value in this text box specifies the number of minutes (if any) after which the router should create an event in the event log that states that the interface has been active for this period.

Limit the data transmitted over this interface
When checked, this checkbox reveals the following parameters that control what data volume restrictions (if any) should be applied to this interface:

Issue a warning event after n units
The value in this text box is the amount of traffic which will cause a warning event to be generated in the event log stating that the specified amount of data has been transferred. The units are specified by a drop-down list, having the following options; KBytes, MBytes, GBytes. For example, if the monthly tariff includes up to 5MB of data before excess usage charges are levied, it would be useful to set this threshold to 4MB.

This would cause the router to create a warning entry in the event log once 4MB of data had been transferred. This event could then be used to trigger an email alert, SNMP trap or SMS alert message.

Stop data from being transmitted after n units
The value in this text box specifies the total amount of data that may be transmitted by this PPP instance before the link is blocked for further traffic, and the value in the drop-down list specifies the units which are; KBytes, MBytes, GBytes.

Reset the data limit on the n day of the month
The value in this text box defined the day of the month on which the data limit is reset to zero.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	metric	0 - 255	Metric
ppp	n	aodion	0 – 2 0 = disabled 1 = enabled 2 = On and return to service immediately	Enable “Always On” mode of this interface, On, On and return to service immediately
ppp	n	immoos	ON, OFF	Put this interface “Out of Service” when an always-on connection attempt fails
ppp	n	aodi_dly	0 – 2147483647	Attempt to reconnect after s seconds
ppp	n	aodi_dly2	0 – 2147483647	If an inhibited PPP interface is connected, attempt to re-connect after s seconds
ppp	n	pwr_dly	0 – 2147483647	Wait s seconds after power-up before activating this interface
ppp	n	tband	0 - 4	Control when this interface can connect using Time Band n
ppp	n	minup	0 – 2147483647	Keep this interface up for at least s seconds
ppp	n	maxup	0 – 2147483647	Close this interface after s seconds
ppp	n	maxuptime	0 – 2147483647	if it has been up for m minutes in a day
ppp	n	timeout	0 – 2147483648	if the link has been idle for s seconds
ppp	n	timeout2	0 – 2147483648	Alternative idle timer for static routes s seconds
ppp	n	rxtimeout	0 – 2147483648	if the link has not received any packets for s seconds

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	maxneg	0 – 2147483648	if the negotiation is not complete in s seconds
ppp	n	uplogmins	0 – 2147483647	Generate an event after this interface has been up for m mins
ppp	n	dlwarnkb	0 – 2147483647	Issue a warning after n units
ppp	n	dlstopkb	0 – 2147483647	Stop data from being transmitted after n units
ppp	n	dlrstday	0 – 255	Reset the data limit on the n day of the month

LAPD > LAPDn

Configuration - Network > Interfaces > ISDN> LAPD> LAPDn

This page allows you to configure the ISDN LAPD interfaces. Link Access Protocol D (LAPD) is the protocol used for ISDN D-channel signalling and call setup.

LAPD 0 and LAPD 1 can be used as required for SAPI 16 traffic (i.e. X.25 over D-channel). LAPD 2 is normally reserved for ISDN call control.

Enable LAPD n

Un-checking this parameter will disable the LAPD instance. This may be necessary if you have an installation where two or more units are connected to the same ISDN "S" bus. In this case, only one of the units may be configured for D-channel X.25 on TEI1, SAPI16. On each of the other units you must disable any LAPD instance for which the TEI is set to 1 in order to prevent it from responding to X.25 traffic on that TEI that is actually destined for another unit.
When checked, this check box will also reveal the following configuration parameters

Mode

When the DTE/DCE mode parameter is set to DTE, the unit will behave as a DTE. This is the default value and should not be changed for normal operation across the ISDN network. If your application involves using two units back-to-back, one of the units should have the DTE mode value set to DCE.

N400 Counter

This is the standard LAPB/LAPD retry counter. The default value is 3 and it should not normally be necessary to change this.

RR Timer n msecs

This is a standard LAPB/LAPD "Receiver Ready" timer. The default value is 10,000ms (10 seconds) and it should not normally be necessary to change this.

T1 Timer n msecs

This is the standard LAPB/LAPD timer. The default value is 1000 milliseconds (1 second) and it should not normally be necessary to change this.

T200 Timer n msecs

This is the standard LAPB/LAPD re-transmit timer in milliseconds. The default value is 1000 milliseconds (1 second) and it should not normally be necessary to change this.

TEI

Each ISDN terminal device connected to your ISDN basic rate outlet must be assigned a unique Terminal Endpoint Identifier (TEI). In most cases, this is negotiated automatically. In some cases however, it may be necessary to assign a fixed TEI.
When TEI is set to 255, the TEI is negotiated with the ISDN network. To use a fixed TEI set the TEI parameter to the appropriate value as specified by your service provider.

D-channel X.25 Tx Window Size
This specifies the transmit window size when using D-channel X.25. The default is 7.

Tx Throughput
The Tx Throughput parameter is used in conjunction with the **Rx Throughput** parameter to limit the maximum data throughput on a LAPD link in bits per second.
If this parameter is set to 0, the unit will transmit data across the LADP link as fast as possible whilst observing hardware or software flow control if enabled.
When set to a value greater than 0, the unit will limit the rate at which data is transmitted over the LAPD link.

Note:
Note that if multiple PAD or IP instances are sharing this LAPD instance, the maximum transmission rates of all instances will be limited.

Rx Throughput
The Rx Throughput parameter is used in conjunction with the **Tx Throughput** parameter to limit the maximum data throughput on a LAPD link in bits per second.
If this parameter is set to 0, the unit will transmit data across the LADP link as fast as possible whilst observing hardware or software flow control if enabled.
When set to a value greater than 0, the unit will limit the rate at which data can be received over the LAPD link when it detects that receive throughput exceeds the specified rate

Note:
Note that if multiple PAD or IP instances are sharing this LAPD instance, the maximum transmission rates of all instances will be limited.

Reactivate D-channel connection

When this parameter is enabled, the unit will try to reactivate a D-channel connection after disconnection by the network by transmitting SABME frames. If it is unable to reactivate the connection after retrying the number of times specified by the N400 counter, it will wait for 1 minute before repeating the retry sequence.

Enabling this parameter also deactivates the **Reactivate after n secs** parameter

If this parameter is disabled, the unit will not attempt to reactivate a D-channel link following deactivation by the network.

Reactivate after n secs
This parameter specifies the number of seconds a deactivation has to be present before the LAPD instance will try to reactivate itself.

After X.25 PAD session is terminated
This parameter determines if to deactivate or not the LAPD session when an X.25 PAD session is terminated

Deactivate the LAPD session
This parameter enables automatic deactivation of a LAPD session when an X.25 PAD session is terminated.

Do not deactivate the LAPD session
This parameter ensures the unit will not deactivate the LAPD session when an X.25 PAD session is terminated.

Enable D64S Mode
D64S mode is a mode in which ISDN B-channel(s) may be used without the need to use any D channel protocol. It is sometimes referred to as “nailed up” ISDN. To enable this mode for this LAPD instance, Tick the D64S mode parameter checkbox and ensure that the **TEI** parameter is set to 255. This means that for any application that uses ISDN (e.g. PPP) then it will use D64S mode.

First D64S B-channel
When using D64S mode there is no dialling protocol to negotiate which B-channel to use. This must therefore be specified using this parameter. Check B1 radio button to select channel B1 and Check B2 radio button to select channel B2 (if another channel is requested from an application then it will use the other unused B channel).

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
LAPD	n	enabled	off, on	Enable LAPD n
LAPD	n	dtemode	off, on	Mode
LAPD	n	n400	1 - 255	N400 Counter
LAPD	n	tnoact	1000 - 60000	RR Timer n msecs
LAPD	n	t1time	1 - 60000	T1 Timer n msecs
LAPD	n	t200	1 – 60000	T200 Timer n msecs
LAPD	n	tei	0 - 255	TEI
LAPD	n	window	1 - 7	D-channel X.25 Tx Window Size
LAPD	n	tthruput	0 - 1410065407	Tx Throughput
LAPD	n	rthruput	0 - 1410065407	Rx Throughput
LAPD	n	keepact	off, on	Reactivate D-channel connection
LAPD	n	reactsecs	0 - 2147483647	Reactivate after n secs
LAPD	n	nodeact	off	After X.25 PAD session is terminated: Deactivate the LAPD session
LAPD	n	nodeact	on	After X.25 PAD session is terminated: Do not deactivate the LAPD session
LAPD	n	d64smode	off, on	Enable D64S Mode
LAPD	n	d64schan	1, 2	First D64S B-channel: B1, B2

PSTN

Configuration – Network > Interfaces > PSTN

This section of the web interface appears when the router is fitted with an optional internal PSTN MODEM card. When first powered up, navigating to the ***Configuration – Network > Interfaces > PSTN*** page will show a message indicating that the MODEM card does not have a PPP instance associated with it. Follow the link on the page and select an unassigned PPP interface to the MODEM. When the browser is refreshed and the ***Configuration – Network > Interfaces > PSTN*** page redisplayed, it should show the parameters described below, along with a message at the top of the page indicating which PPP instance has been selected.

This PSTN interface is using PPP n
This message simply states which PPP instance has been assigned to the interface.

Description
The value in this text box is a memorable name for the interface. This may be useful when referring to the interface, rather than having to remember the name and the function of the interface.

Dial out using numbers
These four text boxes contain the telephone numbers that should be used, in sequence, to make an outgoing connection.

Prefix n to the dial out number
The value in this text box specifies the dialling prefix to use, if needed. This may be necessary when using a PABX.

Username
The text string text box is the username that should be used when using the PPP instance to connect to the remote peer. This will normally be provided by an ISP for use with a dial-in Internet access service.

Password
This text box contains the password to use for authenticating the remote peer and is used in conjunction with the above username.

Confirm password
Type the password into this text box to enable the router to confirm that the password has been entered identically in both boxes.

Allow the remote device to assign a local IP address to this router

When this radio button is selected, the remote peer will assign this PPP interface an IP address.

Try to negotiate a.b.c.d as the local IP address for this router

If it would be useful, but not essential, to have a predefined IP address for the interface, the second radio button should be selected and the desired IP address entered into the text box to the right.

Use a.b.c.d as the local IP address for this router

If it is essential that the PPP interface has a specific IP address, this radio button should be selected and the IP address entered into the text box.

Use the following DNS servers if not negotiated

Primary DNS server
The value in this text box is the IP address of the primary DNS server to use if a DNS server is not assigned as part of the PPP negotiation and connection process. It is fairly common practice for the DNS server to be assigned automatically by the ISP when making a connection.

Secondary DNS server
The value in this text box specifies the IP address of the secondary DNS server to use if one is not automatically assigned by the remote peer.

Attempt to assign the following IP configuration to remote devices
When checked, this check box will reveal the following four configuration parameters which control how the PPP instance assigns an IP address to a connecting remote peer. The primary and secondary DNS server addresses will also be sent to the remote peer

Assign remote IP addresses from a.b.c.d to a.b.c.d
The IP addresses in these text boxes define the pool of IP addresses to assign to remote peers during the IP protocol configuration phase of the PPP negotiation process.

Primary DNS server
The value in this text box is the IP address of the primary DNS server that the remote peer should use when making DNS requests over the link.

Secondary DNS server
The value in this text box is the IP address of the secondary DNS server that the remote peer should use when making DNS requests, should the primary server be unavailable.

Allow the PPP interface to answer incoming calls
When checked, this checkbox will cause the PPP instance to answer an incoming call.

Only allow calling numbers ending with n
When set to answer calls, the value in this textbox provides a filter for ISDN sub-addresses. This value is blank by default but when the PPP instance is set to answer calls, only numbers having trailing digits that match the sub-address value in this test will be answered. So for example, if this value is set to “123”, only calls from numbers with trailing digits that match this value will be answered. For example 01942 605123

Enable NAT on this interface
When checked, this checkbox will enable Network Address Translation to operate on this interface. This is the same as for other PPP interfaces.

IP address / IP address and Port
These radio buttons select whether IP address translation only should be applied or whether port number translation should also be applied to IP packets.

Enable IPsec on this interface
When checked, this checkbox will cause the router to encrypt traffic on this interface using the IPsec protocol. The following two additional configuration parameters are revealed when this box is checked.

Keep Security Associations (SAs) when this PSTN interface is disconnected
When checked, this checkbox causes the router to maintain (i.e. not flush) the SA when the interface becomes disconnected. The normal behaviour is to remove the SAs when the interface becomes disconnected.

Use interface x,y for the source IP address of IPsec packets
If it is required to use another interface (i.e. not the interface currently being configured) as the source address for IPsec packets, this may be achieved by selecting the desired interface from the drop-down list and typing the desired interface instance number into the adjacent text box.

Enable the firewall on this interface
When checked, this checkbox applies the firewall rules to traffic using this interface.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	name	Up to 25 characters	Description
ppp	n	phonenum	up to 25 digits	Dial out using numbers
ppp	n	ph2	"	"
ppp	n	ph3	"	"
ppp	n	ph4	"	"
ppp	n	prefix	0 – 9999999999	Prefix n to the dial out number
ppp	n	username	Up to 60 characters	Username
ppp	n	password	Up to 40 characters	Password
ppp	n	IPaddr	0.0.0.0	Allow the remote device to assign a local IP address to this router
ppp	n	IPaddr	Valid IP address a.b.c.d	Try to negotiate a.b.c.d as the local IP address for this router (in conjunction with l_addr)
ppp	n	l_addr	OFF,ON When ON, allows negotiation when OFF force use of specified IP address	Use a.b.c.d as the local IP address of this router
ppp	n	DNSserver	Valid IP address a.b.c.d	Use the following DNS servers if not negotiated Primary DNS server a.b.c.d
ppp	n	secDNS	Valid IP address a.b.c.d	Use the following DNS servers if not negotiated Secondary DNS server a.b.c.d
ppp	n	IPmin	Valid IP address a.b.c.d	Assign remote IP addresses from a.b.c.d to a.b.c.d
ppp	n	IPrange	0 - 255	Assign remote IP addresses from a.b.c.d to a.b.c.d
ppp	n	transDNS	Valid IP address	Primary DNS server a.b.c.d

Entity	Instance	Parameter	Values	Equivalent Web Parameter
			a.b.c.d	
ppp	n	sectransDNS	Valid IP address a.b.c.d	Secondary DNS server a.b.c.d
ppp	n	ans	OFF,ON	Allow this PPP interface to answer incoming calls
ppp	n	cingnb	up to 25 digits	Only allow calling numbers ending with n
ppp	n	do_nat	0,1,2 0 = Disabled 1 = IP address 2 = IP address and port	Enable NAT on this interface IP address/IP address and Port
ppp	n	nat_ip	Valid IP address a.b.c.d	NAT Source IP address a.b.c.d
ppp	n	ipsec	0 = Disabled 1 = Enabled 2 = Enabled and Keep SAs	Enable IPsec on this interface/ Keep Security Associations when this PSTN interface is disconnected
ppp	n	firewall	OFF,ON	Enable the firewall on this interface

Advanced

Configuration – Network > Interfaces > PSTN> Advanced

Metric
The value in this text box specifies the route metric that should be applied to this interface. (see ***Configuration – Network > Interfaces > Advanced > PPP n*** for more detail.)

Enable "Always On" mode of this interface
When checked, this checkbox causes the following two options to appear:

On / On and return to service immediately
These two radio buttons select whether the "always-on" functionality should simply be enabled or whether the additional facility to return the interface to the "In Service" state should be applied.

Put this interface "Out of Service" when an always-on connection attempt fails
Normally, always-on interfaces will not go out of service unless they have connected at least once. When checked, this checkbox causes the router to put the interface out of service even if the first connection attempt fails.

Attempt to re-connect after s seconds
The parameter in this text box specifies the length of time in seconds that the router should wait after an "always-on" PPP connection has been terminated before trying to re-establish the link.

If an inhibited PPP interface is connected, attempt to re-connect after s seconds
The value in this text box takes precedence over the previous parameter when another PPP instance that is usually inhibited by this one is connected. This parameter would

typically be used to reduce the connection retry rate when a lower priority PPP instance is connected.

Wait s seconds after power-up before activating this interface
The value in this text box is the initial delay that the router will apply before activating the PPP instance after power-up. After the initial power-up delay the normal always-on activation timers apply. When set to zero, no delay will be applied.

Control when this interface can connect using Time band n
These two controls, the check box and drop-down list determine whether the Time Band function should be applied to this interface. Checking the checkbox enables the functionality and the desired time band instance is selected from the drop-down list. Time Band functionality is explained in the ***Configuration – Network > Interfaces > Timebands*** section of this manual.

Keep this interface up for at least s seconds
The value in this textbox specifies the minimum period that the PPP interface should remain available. This means that even if the link becomes inactive before this period expires, the connection will remain open.

Close this interface

After s seconds
The value in this text box specifies the maximum time that the link will remain active in any one session. After this time, the link will be deactivated.

If it has been up for m minutes in a day
The router will deactivate the PPP instance after it has been active for the value specified in this text box.

If the link has been idle for s seconds
The router will deactivate this interface after the time specified in this text box if it detects that the link has not passed any traffic for that period.

Alternative idle timer for static routes s seconds
The value in this text box specifies an alternative inactivity timeout for use in conjunction with the "Make PPP n interface use the alternative idle timeout when this route becomes available" parameter on the ***Configuration – Network > IP Routing/Forwarding > Static Routes > Routes n > Advanced*** web page. This timeout will only be used until the PPP instance next deactivates. After that the normal timeout value is used.

If the link has not received any packets for s seconds
The value in this text box specifies the amount of time that the router will wait without receiving any PPP packets before disconnecting. The timer is reset with each received PPP packet.

If the negotiation is not complete in s seconds
The value in this textbox specifies the maximum time (in seconds) allowed for the PPP negotiation to complete. If negotiations have not completed within this period, the interface is deactivated.

Generate an event after this interface has been up for m minutes
The value in this text box specifies the number of minutes (if any) after which the router should create an event in the event log that states that the interface has been active for this period.

Limit the data transmitted over this interface
When checked, this checkbox reveals the following parameters that control what data volume restrictions (if any) should be applied to this interface:

Issue a warning event after n units
The value in this text box is the amount of traffic which will cause a warning event to be generated in the event log stating that the specified amount of data has been transferred. The units are specified by a drop-down list, having the following options; KBytes, MBytes, GBytes. For example, if the monthly tariff includes up to 5MB of data before excess useage charges are levied, it would be useful to set this threshold to 4MB. This would cause the router to create a warning entry in the event log once 4MB of data had been transferred. This event could then be used to trigger an email alert, SNMP trap or SMS alert message.

Stop data from being transmitted after n units
The value in this text box specifies the total amount of data that may be transmitted by this PPP instance before the link is blocked for further traffic, and the value in the drop-down list specifies the units which are; KBytes, MBytes, GBytes.

Reset the data limit on the n day of the month

The value in this text box defined the day of the month on which the data limit is reset to zero.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	metric	0 - 255	Metric
ppp	n	aodion	0 – 2 0 = disabled 1 = enabled 2 = On and return to service immediately	Enable “Always On” mode of this interface, On, On and return to service immediately
ppp	n	immoos	ON, OFF	Put this interface “Out of Service” when an always-on connection attempt fails
ppp	n	aodi_dly	0 – 2147483647	Attempt to reconnect after s seconds
ppp	n	aodi_dly2	0 – 2147483647	If an inhibited PPP interface is connected, attempt to re-connect after s seconds
ppp	n	pwr_dly	0 – 2147483647	Wait s seconds after power-up before activating this interface
ppp	n	tband	0 - 4	Control when this interface can connect using Time Band n
ppp	n	minup	0 – 2147483647	Keep this interface up for at least s seconds
ppp	n	maxup	0 – 2147483647	Close this interface after s seconds
ppp	n	maxuptime	0 – 2147483647	if it has been up for m minutes in a day
ppp	n	timeout	0 – 2147483648	if the link has been idle for s

Entity	Instance	Parameter	Values	Equivalent Web Parameter
				seconds
ppp	n	timeout2	0 – 2147483648	Alternative idle timer for static routes s seconds
ppp	n	rxtimeout	0 – 2147483648	if the link has not received any packets for s seconds
ppp	n	maxneg	0 – 2147483648	if the negotiation is not complete in s seconds
ppp	n	uplogmins	0 – 2147483647	Generate an event after this interface has been up for m mins
ppp	n	dlwarnkb	0 – 2147483647	Issue a warning after n units
ppp	n	dlstopkb	0 – 2147483647	Stop data from being transmitted after n units
ppp	n	dlrstday	0 – 255	Reset the data limit on the n day of the month

DialServ

Configuration – Network > Interfaces > DialServ

The Dialserv option module mimics a telephone exchange in that it supplies the required voltages on the line, generates a RING signal and has off-hook detection circuitry. It can be used to provide similar functionality to dialling into an ISP using an analogue MODEM. The card also contains an analogue MODEM to handle data on the line.

Use PPP / Protocol Switch
These radio buttons select whether the DialServ card uses a PPP instance or the protocol switch functionality to control traffic on the interface. If PPP is selected, the web page expands to reveal the standard PPP configuration settings. If Protocol Switch is selected, only the four settings described immediately below are visible.

Max time to RING line s seconds
The value in this text box specifies the maximum number of seconds that the RING signal should be generated for.

RING frequency n Hz
The DialServer module generates a RING signal – the frequency of the RING is selected from this drop-down list. The available options are:

- 20Hz
- 25Hz
- 30Hz
- 40Hz
- 50Hz.

Initialisation string 1
The text string in this text box contains any required MODEM initialisation commands.

Initialisation string 2
The text string in this text box contain initialisation commands that will be issued to the MODEM after the first initialisation string.

DialServ Network Settings

Configuration – Network > Interfaces > DialServ> DialServ Network Settings

The DialServ card may be configured to use PPP as the protocol to connect to the remote peer and as such should be assigned a free PPP instance to use as part of the configuration. If no PPP instance has been assigned and the module has been configured to use PPP, a link to the PPP mappings page and message appear.
If a PPP instance has been assigned, the following configuration options appear:

This DialServ interface is using PPP n
This message simply indicates which PPP instance (n) is being used by the DialServ card.

Description
The value in this text box is a short string that describes the interface and is used as a convenience when referring to the interface.

Dial out using numbers
These four text boxes contain the telephone numbers that should be used, in sequence, to make an outgoing connection. These can be used to provide a dialback facility.

Prefix n to the dial out number
The value in this text box specifies the dialling prefix to use, if needed. This may be necessary when using a PABX.

Username
The text string text box is the username that should be used when using the PPP instance to connect to the remote peer.

Password
This text box contains the password to use for authenticating the remote peer and is used in conjunction with the above username.

Confirm Password
Type the password into this text box to enable the router to confirm that the password has been entered identically in both boxes.

Allow the remote device to assign a local IP address to this router

When this radio button is selected, the remote peer will assign this PPP interface an IP address.

Try to negotiate a.b.c.d as the local IP address for this router

If it would be useful, but not essential, to have a predefined IP address for the interface, the second radio button should be selected and the desired IP address entered into the text box to the right.

Use a.b.c.d as the local IP address for this router

If it is essential that the PPP interface has a specific IP address, this radio button should be selected and the IP address entered into the text box.

Use the following DNS servers if not negotiated

Primary DNS server
The value in this text box is the IP address of the primary DNS server to use if a DNS server is not assigned as part of the PPP negotiation and connection process. It is fairly common practice for the DNS server to be assigned automatically by the ISP when making a connection.

Secondary DNS server
The value in this text box specifies the IP address of the secondary DNS server to use if one is not automatically assigned by the remote peer.

Attempt to assign the following IP configuration to remote devices
When checked, this check box will reveal the following four configuration parameters which control how the PPP instance assigns an IP address to a connecting remote peer. The primary and secondary DNS server addresses will also be sent to the remote peer

Assign remote IP addresses from a.b.c.d to a.b.c.d
The IP addresses in these text boxes define the pool of IP addresses to assign to remote peers during the IP protocol configuration phase of the PPP negotiation process.

Primary DNS server
The value in this text box is the IP address of the primary DNS server that the remote peer should use when making DNS requests over the link.

Secondary DNS server
The value in this text box is the IP address of the secondary DNS server that the remote peer should use when making DNS requests, should the primary server be unavailable.

Allow the PPP interface to answer incoming calls
When checked, this checkbox will cause the PPP instance to answer an incoming call.

Only allow calling numbers ending with n
When set to answer calls, the value in this textbox provides a filter for ISDN sub-addresses. This value is blank by default but when the PPP instance is set to answer calls, only numbers having trailing digits that match the sub-address value in this test will be answered. So for example, if this value is set to “123”, only calls from numbers with trailing digits that match this value will be answered. For example 01942 605123

Enable NAT on this interface
When checked, this checkbox will enable Network Address Translation to operate on this interface. This is the same as for other PPP interfaces.

IP address / IP address and Port
These radio buttons select whether IP address translation only should be applied or whether port number translation should also be applied to IP packets.

Enable IPsec on this interface
When checked, this checkbox will cause the router to encrypt traffic on this interface using the IPsec protocol. The following two additional configuration parameters are revealed when this box is checked.

Keep Security Associations (SAs) when this PSTN interface is disconnected
When checked, this checkbox causes the router to maintain (i.e. not flush) the SA when the interface becomes disconnected. The normal behaviour is to remove the SAs when the interface becomes disconnected.

Use interface x,y for the source IP address of IPsec packets
If it is required to use another interface (i.e. not the interface currently being configured) as the source address for IPsec packets, this may be achieved by selecting the desired interface from the drop-down list and typing the desired interface instance number into the adjacent text box.

Enable the firewall on this interface
When checked, this checkbox applies the firewall rules to traffic using this interface.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	name	Up to 25 characters	Description
ppp	n	phonenum	up to 25 digits	Dial out using numbers
ppp	n	ph2	“	Dial out using numbers
ppp	n	ph3	“	Dial out using numbers
ppp	n	ph4	“	Dial out using numbers
ppp	n	prefix	0 – 9999999999	Prefix
ppp	n	username	Up to 60 characters	Username
ppp	n	password	Up to 40 characters	Password
ppp	n	IPaddr	0.0.0.0	Allow the remote device to assign a local IP address to this router
ppp	n	IPaddr	Valid IP address a.b.c.d	Try to negotiate a.b.c.d as the local IP address for this router (in conjunction with l_addr)
ppp	n	l_addr	OFF,ON When ON, allows negotiation when OFF force use of specified IP address	Use a.b.c.d as the local IP address for this router (not negotiable)
ppp	n	DNSserver	Valid IP address a.b.c.d	Primary DNS server
ppp	n	secDNS	Valid IP address a.b.c.d	Secondary DNS server
ppp	n	IPmin	Valid IP address a.b.c.d	Assign remote IP addresses from a.b.c.d to a.b.c.d
ppp	n	IPrange	0 - 255	Assign remote IP addresses from a.b.c.d to a.b.c.d
ppp	n	transDNS	Valid IP address a.b.c.d	Primary DNS server a.b.c.d
ppp	n	sectransDNS	Valid IP address a.b.c.d	Secondary DNS server a.b.c.d
ppp	n	ans	OFF,ON	Allow this PPP interface to answer incoming calls
ppp	n	do_nat	0,1,2 0 = Disabled 1 = IP address 2 = IP address and port	Enable NAT on this interface IP address/IP address and Port

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	natip	Valid IP address a.b.c.d	NAT Source IP address a.b.c.d
ppp	n	ipsec	0 = Disabled 1 = Enabled 2 = Enabled and Keep SAs	Enable IPsec on this interface/ Keep Security Associations when this DialServ interface is disconnected
ppp	n	firewall	OFF,ON	Enable the firewall on this interface

Advanced

Configuration – Network > Interfaces > DialServ> DialServ Network Settings> Advanced

Metric
The value in this text box specifies the route metric that should be applied to this interface. (see ***Configuration – Network > Interfaces > Advanced > PPP n*** for more detail.)

Enable "Always On" mode of this interface
When checked, this checkbox causes the following two options to appear:

On / On and return to service immediately
These two radio buttons select whether the "always-on" functionality should simply be enabled or whether the additional facility to return the interface to the "In Service" state should be applied.

Put this interface "Out of Service" when an always-on connection attempt fails.
Normally, always-on interfaces will not go out of service unless they have connected at least once. When checked, this checkbox causes the router to put the interface out of service even if the first connection attempt fails.

Attempt to re-connect after s seconds
The parameter in this text box specifies the length of time in seconds that the router should wait after an "always-on" PPP connection has been terminated before trying to re-establish the link.

If an inhibited PPP interface is connected, attempt to re-connect after s seconds
The value in this textbox takes precedence over the previous parameter when another PPP instance that is usually inhibited by this one is connected. This parameter would typically be used to reduce the connection retry rate when a lower priority PPP instance is connected.

Wait s seconds after power-up before activating this interface
The value in this textbox is the initial delay that the router will apply before activating the PPP instance after power-up. After the initial power-up delay the normal always-on activation timers apply. If set to zero, no delay will be applied.

Control when this interface can connect using Time band n
These two controls, the check box and drop-down list determine whether the Time Band function should be applied to this interface. Checking the checkbox enables the functionality and the desired time band instance is selected from the drop-down list. Time Band functionality is explained in the ***Configuration – Network > Interfaces > Timebands*** section of this manual.

Keep this interface up for at least s seconds

The value in this textbox specifies the minimum period that the PPP interface should remain available. This means that even if the link becomes inactive before this period expires, the connection will remain open.

Close this interface

after s seconds
The value in this text box specifies the maximum time that the link will remain active in any one session. After this time, the link will be deactivated.

If it has been up for m minutes in a day
The router will deactivate the PPP instance after it has been active for the value specified in this text box.

If the link has been idle for s seconds
The router will deactivate this interface after the time specified in this text box if it detects that the link has not passed any traffic for that period.

Alternative idle timer for static routes s seconds
The value in this text box specifies an alternative inactivity timeout for use in conjunction with the "Make PPP n interface use the alternative idle timeout when this route becomes available" parameter on the ***Configuration – Network > IP Routing/Forwarding > Static Routes > Routes n > Advanced*** web page. This timeout will only be used until the PPP instance next deactivates. After that the normal timeout value is used.

If the link has not received any packets for s seconds
The value in this text box specifies the amount of time that the router will wait without receiving any PPP packets before disconnecting. The timer is reset with each received PPP packet.

If the negotiation is not complete in s seconds
The value in this textbox specifies the maximum time (in seconds) allowed for the PPP negotiation to complete. If negotiations have not completed within this period, the interface is deactivated.

Generate an event after this interface has been up for m minutes
The value in this text box specifies the number of minutes (if any) after which the router should create an event in the event log that states that the interface has been active for this period.

Limit the data transmitted over this interface
When checked, this checkbox reveals the following parameters that control what data volume restrictions (if any) should be applied to this interface:

Issue a warning event after n units
The value in this text box is the amount of traffic which will cause a warning event to be generated in the event log stating that the specified amount of data has been transferred. The units are specified by a drop-down list, having the following options; KBytes, MBytes, GBytes. For example, if the monthly tariff includes up to 5MB of data before excess useage charges are levied, it would be useful to set this threshold to 4MB. This would cause the router to create a warning entry in the event log once 4MB of data had been transferred. This event could then be used to trigger an email alert, SNMP trap or SMS alert message.

Stop data from being transmitted after n units
The value in this text box specifies the total amount of data that may be transmitted by this PPP instance before the link is blocked for further traffic, and the value in the drop-down list specifies the units which are; KBytes, MBytes, GBytes.

Reset the data limit on the n day of the month

The value in this text box defined the day of the month on which the data limit is reset to zero.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	metric	0 - 255	Metric
ppp	n	aodion	0 – 2 0 = disabled 1 = enabled 2 = On and return to service immediately	Enable “Always On” mode of this interface, On, On and return to service immediately
ppp	n	immoos	ON, OFF	Put this interface “Out of Service” when an always-on connection attempt fails
ppp	n	aodi_dly	0 – 2147483647	Attempt to reconnect after s seconds
ppp	n	aodi_dly2	0 – 2147483647	If an inhibited PPP interface is connected, attempt to re-connect after s seconds
ppp	n	pwr_dly	0 – 2147483647	Wait s seconds after power-up before activating this interface
ppp	n	tband	0 - 4	Control when this interface can connect using Time Band n
ppp	n	minup	0 – 2147483647	Keep this interface up for at least s seconds
ppp	n	maxup	0 – 2147483648	Close this interface after s seconds
ppp	n	maxuptime	0 – 2147483647	if it has been up for m minutes in a day
ppp	n	timeout	0 – 2147483648	if the link has been idle for s seconds
ppp	n	timeout2	0 – 2147483648	Alternative idle timer for static routes s seconds
ppp	n	rxtimeout	0 – 2147483648	if the link has not received any packets for s seconds
ppp	n	maxneg	0 – 2147483648	if the negotiation is not complete in s seconds
ppp	n	uplogmins	0 – 2147483647	Generate an event after this interface has been up for m mins
ppp	n	dlwarnkb	0 – 2147483647	Issue a warning after n units
ppp	n	dlstopkb	0 – 2147483647	Stop data from being

Entity	Instance	Parameter	Values	Equivalent Web Parameter
				transmitted after n units
ppp	n	dlrstday	0 – 255	Reset the data limit on the n day of the month
pots	0	connect_secs	x	Number of seconds maximum to wait for the modem to connect

Serial

Configuration – Network > Interfaces > Serial

Digi routers support a variety of serial interfaces, either inbuilt or as optional add-on modules. Each asynchronous serial (ASY) port may be configured to operate at different speed, data format etc. These parameters may be changed using the web interface or from the command line using AT commands and S registers.

The ***Configuration – Network > Interfaces > Serial*** menu item opens out when clicked, to show the list of supported serial interfaces.

Note:
On models fitted with W-WAN modules, one of the interfaces (and its associated web page) will be dedicated to the W-WAN module. The title will reflect this. Similarly, on models fitted with an analogue MODEM, one of the interfaces will be entitled PSTN port.

The ***Configuration – Network > Interfaces > Serial*** menu has the following sub-menu options:

- Serial Port n
- Sync Rate Adaption
- Command Mappings
- Protocol Bindings
- TRANSIP Serial Ports
- RealPort
- Multitx

Serial Port n

Configuration – Network > Interfaces > Serial> Serial Port n

This section describes the basic configuration of a serial port.

Enable this serial interface
When this checkbox is unchecked, this is the only item that appears in the section. Clicking the checkbox causes the various associated configuration parameters to appear.

Description
This free-form text entry box allows a description for the interface to be added. For example, if the serial interface is connected to a card payment device, the description could read “Till 1” or similar appropriate text.

Baud Rate
This drop-down selection box selects the required Baud rate for the associated serial port.

Data Bits / Parity
This drop-down selection box selects the required data format for the interface, 8 data bits, no parity being a very common configuration.

Note:
When the serial port is not in 8-bit parity mode (i.e. it is in either 8-bit no parity, or 7-bit with parity), the router will continually check for parity when receiving AT commands and adjust and match accordingly.

Flow Control
The unit supports software flow control using XON/XOFF characters and hardware flow control using the RS232 RTS and CTS signals. Use this drop-down list to select "Software", "Hardware" or a combination of "Both". To disable flow control select the "None" option.

Enable echo on this interface
Check this checkbox to enable command echo to be enabled when using the command line interpreter, uncheck it if the attached terminal provides local echo.

CLI result codes
Select the required level of verbosity for command result codes. The available options are:

- Verbose
- Numeric
- None.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
asy	n/a	descr	Free text – description of interface	Description
S31=n	n/a	n/a	Where n = 3 = 115200 4 = 57600 5 = 38400 6 = 19200 7 = 9600 8 = 4800	Baud rate
S23=n	n/a	n/a		Data Bits / Parity
&Kn	n/a	n/a	Where n = 0 = None 1 = Hardware 2 = Software 3 = Both	Flow Control
&En	n/a	n/a	Where n = 0 = No echo 1 = echo	Enable echo on this interface
&Vn	n/a	n/a	Where n = 0 = numeric 1 = verbose	CLI result codes

Advanced

Configuration – Network > Interfaces > Serial> Serial Port n> Advanced

The configuration parameters in this section are changed less frequently than those in the basic section and so are given a separate page in order to reduce screen clutter.

Answer V.120 calls after n rings (0 = Don't answer)
This parameter controls the answering of incoming V.120 calls. When set to zero, V.120 answering is disabled, otherwise V.120 answering is enabled on this interface. Enter the number of rings to wait before answering the call into this text box. This is equivalent to setting the value of the "S0" register for the associated serial port.

DCD
This drop-down selection box selects how the Data Carrier Detect (DCD) signal is controlled. The available options are:
Auto
On
Off
Pulse Low.
Selecting "Auto" configures the router so that it will only assert the DCD line when an ISDN connection has been established (this is equivalent to "AT&C1").
Selecting "On" configures the router such that the DCD line is always asserted when the router is powered-up (this is equivalent to "AT&C0").
Selecting "Off" configures the router such that the DCD line is normally asserted but is de-asserted for the time period specified by the "S10" register after a call is disconnected (this is equivalent to "AT&C2").

DTR Control
This drop-down selection box controls how the router responds to the DTR signal. The available options are:

- None
- Drop call
- Drop line and call
- Drop call on transition
- Drop line & call on transition.

Selecting "None" configures the router to ignore the DTR signal (this is equivalent to "AT&D0").
Selecting "Drop call" configures the router to disconnect the current call and return to AT command mode when the DTR signal from the attached terminal (DTE) is de-asserted (this is equivalent to "AT&D1").
Selecting "Drop line and call" configures the router to disconnect the current call, drop the line and return to AT command mode when the DTR signal is de-asserted (this is equivalent to "AT&D2").

DTR de-bounce time s x 20 milliseconds
This parameter determines the length of time (in multiples of 20ms) for which the DTR signal must be de-asserted before the router acts on any options that are set to trigger on loss of this signal. Enter the desired multiple into the text box. Increasing this value makes the router less sensitive to "bouncing" of the DTR signal. Conversely, decreasing this value makes the router more sensitive. The default of 100ms (5 times 20ms) is a reasonable value.

Escape Character

This parameter determines the character used in the escape sequence. The default is the "+" symbol (ASCII value 43, 0x2b). Changing this value has the same effect as changing the "S2" register.

Escape Delay s x 20 milliseconds
This parameter defines the required minimum length of the pause (in multiples of 20ms) in the escape sequence. The default is 50 x 20ms which means that the escape sequence becomes "+++", a pause of 1 second and then "AT" in order to drop back to AT command mode. Enter the desired delay into the text box if a delay of some other value is required.

Forwarding Timeout s x 10 milliseconds
This parameter defines the length of time that the router will wait for more data after receiving at least one octet of data through the serial port and transmitting it onwards. This timer is reset each time more data is received. The router will forward data onwards when either the forwarding timer expires or the input buffer becomes full. This parameter applies to ADAPT, TCPDIAL, TCPPERM and PANS.

Break Transmit Escape Character c
This parameter determines the character used in the escape sequence. The "-" symbol (ASCII value 45, 0x2d) is a recommended value. Changing this value has the same effect as changing the "S3" register. To use the break sequence, type "-" 3 times, with a 1 second pause either side of the 3 "-" characters.
When the Async port detects the following sequence....
<guard time 1 sec>---<guard time 1 sec>
instead of outputting the three minus characters (they are removed from the output stream) a BREAK condition is placed on the Async transmitter for 1 second.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
S0=n	n/a	n/a	Where n = 0 - 255	Answer V.120 call after n rings
&Cn	n/a	n/a	Where n = 0 = On 1 = Auto 2 = Off 3 = Pulse low	DCD
&Dn	n/a	n/a	Where n = 0 = None 1 = Drop line 2 = Drop line & call 3 = Drop call on transition 4 = Drop line & call on transition	DTR
S45=n	n/a	n/a	Where n = 0 - 255	DTR de-bounce
S2=n	n/a	n/a	Where n = ASCII value	Escape Character
S12=n	n/a	n/a	Where n = 0 - 255	Escape delay
S15=n	n/a	n/a	Where n =	Forwarding Timeout

Entity	Instance	Parameter	Values	Equivalent Web Parameter
			0 - 255	
S3=n	n/a	n/a	Where n = ASCII value	Break Transmit Escape Character

Profiles

Each serial port can have two profiles which can be configured differently. Which profile is in force when the router powers-up is selected here.

Power-up profile n
Select "0" from the drop-down selection box to choose profile 0 to be active when the router powers-up. Select "1" from the selection box to make profile 1 the active profile.

Load Profile n
Select "0" from the drop-down selection box and click the button to load profile 0.

Save Profile
Select "0" from the drop-down selection box and click the button to save profile 0 after making any changes.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
&Yn			Where n = 0,1	Power-up profile n
&Zn			Where n = 0,1	Load Profile n
&Wn			Where n = 0,1	Save Profile n

Sync

The most common form of serial communications these days is asynchronous. Synchronous serial communications links are still in use and the Digi routers can support these. HDLC is a synchronous protocol that is still in use and can be used with Digi routers. This section describes how to configure the synchronous communications interfaces. To enable synchronous mode, a protocol such as LAPB must be configured to use a synchronous port as its lower layer interface. On certain models, an informational message will appear on the web page which states that jumper settings may need to be changed in order to support synchronous serial operation.

Note:
The number of synchronous serial ports available will vary depending on the model and any optional modules fitted.

Description
This text entry box is for a description of the interface, should one be required.

Clock source Internal / External
These two radio buttons select between internal or external clock sources for the interface.

Mode
The radio buttons that appear here select the specific serial protocol to use. Which buttons appear depend upon the capabilities of the interface. The options available are; V.35, EIA530, RS232, EIA530A, RS449 and X.21.

Invert RX clock
When checked, this checkbox will cause the router to invert the voltage level of the receive clock signal.

Invert TX clock
When checked, this checkbox will cause the router to invert the voltage level of the transmit clock signal.

Encoding NRZ / NRZI
These two radio buttons select between non-return to zero (NRZ) and non-return to zero (inverted) (NRZI) signal encodings.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
sy	0	descr	Text description of interface	Description
sy	0	clksrc	int,ext	Clock source
sy	0	rxclkinv	OFF,ON	Invert RX clock
sy	0	txclkinv	OFF,ON	Invert TX clock
sy	0	encode	nrz,nrzi	Encoding

Rate Adaption

Configuration – Network > Interfaces > Serial> Rate Adaptation

The router supports two rate adaptation protocol (Adapt) instances. Each instance enables the selection and configuration of the protocol to be used for rate adaptation over an ISDN B channel. The supported protocols are; V.110, V.120 and X.75. Depending on which protocol is selected, there may be an associated LAPB instance (distinct from the two general purpose LAPB instances), as for example, when V.120 is used in error-corrected (multi-frame) mode. Clicking the triangle at the left of the blue bar opens up the two instances described below.

Rate Adaption n

Configuration – Network > Interfaces > Serial> Rate Adaptation> Rate Adaptation n

This page displays the configuration parameters directly relevant to the rate adaptation protocol only, LAPB configuration pages are to be found here: ***Configuration – Network > Legacy Protocols > X.25 > LAPB***. When configuring LAPB parameters, be aware that LAPB 2 is used for adapt 0 and LAPB 3 is used for adapt 1.

Attempt to redial the connection n times if rate adaption has not been negotiated
If an ISDN connection is established, but rate adaption is not negotiated, the value in this text box specifies how many times the router should drop the connection and redial it.

Drop the connection if it is idle for h hrs m mins s secs
The values in these text entry boxes specify the time to wait before dropping the connection if the connection becomes idle.

Leased line mode
When checked, this checkbox will allow the router to attempt to maintain the connection automatically once it has been established.

Enable TCP rate adaption
Check this checkbox to enable the use of rate adaptation when using a TCP connection rather than an ISDN line. When enabled, the following controls become enabled:

Connect to IP Address a.b.c.d Port n
When using a TCP connection, these text entry boxes allow the user to specify the IP address and port number that the protocol should use.

Listen on Port
This text entry box contains the port number that the router is listening on when in socket mode.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
adapt	0,1	dial_retries	0 - 255	Attempt to redial the connection n times
adapt	0,1	tinact	0 - 86400	Drop the connection if it is idle for h hrs m mins s secs
adapt	0,1	leased_line	OFF,ON	Leased line mode
adapt	0,1	sockmode	0,1 0 = disable 1 = enable	Enable TCP rate adaption
adapt	0,1	ip_addr	valid IP address a.b.c.d	Connect to IP Address a.b.c.d Port n
adapt	0,1	ip_port	valid TCP port number	Connect to IP Address a.b.c.d Port n
adapt	0,1	lip_port	valid TCP port number	Listen on Port n

Command Mappings

Configuration – Network > Interfaces > Serial> Command Mappings

The router supports a number of command “aliases” which specify strings to be substituted for commands entered at the command line. The table on this page contains two text entry boxes and an “Add” button. Up to 23 command mappings may be specified. An example may make this clear. Suppose, a user coming from a Unix™ background feels more comfortable typing “ls” rather than the native “dir” command in order to list the files in a directory. To achieve this aliasing, enter “ls” into the “From” column in the table, “dir” into the “To” column and then click the “Add” button.

From
This text entry box contains the substitute text.

To
This text entry box contains the command that should be substituted.

Add
Click this button to add the command mapping.

Delete
When the mapping has been added, a “Delete” button will appear in the right-hand column. Clicking this button removes the binding from the table.

Note:
If either string contains spaces, the entire string must be enclosed within double quotation marks. When substituting a command, upper case characters are considered the same as the corresponding lower case characters.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
cmd	n	cmdmapi	Replacement command	From
cmd	n	cmdmapo	Command to be substituted	To

Protocol Bindings

Configuration – Network > Interfaces > Serial> Protocol Bindings

Digi routers are soft configurable to allow different protocols to be used on different interfaces. The process of selecting which protocol will be used on a particular interface is referred to as “binding”. So, for example Serial (ASY) port 0 may be used for an ISDN B channel X.25 connection in which case PAD 0 would be bound to Serial 0 (assuming that PAD 0 is the required PAD). (To complete this example, it would also be necessary to associate the PAD with a LAPB instance using the appropriate page). Protocols are bound to serial interfaces using a table with a drop-down list box for selecting the protocol and a drop-down list for selecting the serial port.

By default, if no specific protocol has been bound to a serial interface, a PPP instance will automatically be associated with that port. This means that PPP is treated as the default protocol associated with the serial ports.

Protocol
Select the desired protocol from this drop-down list.

Bound to
Select the desired serial port from this drop-down list.

Add
Click this button to add the binding.

Delete
When a binding has been added, it appears in the table and a “Delete” button appears in the right-hand column. Click this button to remove the binding. (Remember that the binding does not come into force until the “Apply” button at the bottom of the page has been clicked).

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
bind	n	prot1	Valid protocol, e.g. PAD 0	Protocol
bind	n	id1	Valid serial port e.g. ASY 5	Bound to

To display a list of the current bindings enter the command:

bind ?

Command line examples:

bind pad 0 asy 0

binds PAD 0 to serial port 0.

bind v120 0 asy 3

binds V.120 instance 0 to asynchronous serial port 3.

To access the Internet using PPP via a terminal connected to serial interface 2, enter the command:

bind ppp 1 asy 2

Currently it is only possible to bind a TANS instance to an ADAPT instance using the bind command. The format of the command is:

bind adapt <instance> tans <instance>

TRANSIP Serial Ports

Configuration – Network > Interfaces > Serial> TRANSIP Serial Ports

TransIP is a way of using virtual serial ports for serial connections over an IP socket, in effect multiplying the number of concurrent serial connections to a router. TransIP can be configured to actively connect on a TCP socket (i.e. make outgoing connections).

TRANSIP n

Configuration – Network > Interfaces > Serial> TRANSIP Serial Ports> TRANSIP n

The message at the top of this page states which serial interface is being used for the TransIP connection.

Listen on port n
This parameter is the TCP port number that the router should listen on.

Connect to IP Address or Hostname a.b.c.d Port n
The IP address or hostname text entry box should contain a valid IP address or the hostname which the router should use to make the outgoing TransIP connection.
If this parameter is set (i.e. non-zero), the number defined the TCP port number to use when making TCP socket connections. When zero, TransIP is listening only on the port defined above.

Send TCP Keep-Alives every s seconds
The value in this text entry box is the amount of time (in seconds) a connection will stay open without any traffic being passed.

Enable Stay Connected mode
When checked, this checkbox causes the router to refrain from clearing the TCP socket at the end of a transaction, data call or data session (depending on what the TansIP serial port was bound to and what protocol it was using). Leaving this checkbox unchecked allows the router to clear the socket. For example, if the TransIP port is bound to a TPAD and the box is unchecked, the TransIP TCP socket will be cleared at the end of the TPAD transaction.

Disable command echo
When this checkbox is checked command echo for the TransIP port is disabled. When unchecked all commands issued will be echoed back to the TransIP TCP socket.

Escape char c
The parameter in this text entry box is the ASCII character used as the escape character which is by default "+". Entering this escape character three times followed by a pause of at least the "Escape delay" parameter below and then an "AT" command will cause the router to switch back to command mode from online mode. This is equivalent to the "S2" register setting.

Escape delay s milliseconds
The parameter in this text entry box defines the delay required between entering the escape sequence (default "+++") and the "AT" command in order for the router to drop back into command mode. This is equivalent to the "S12" register setting.

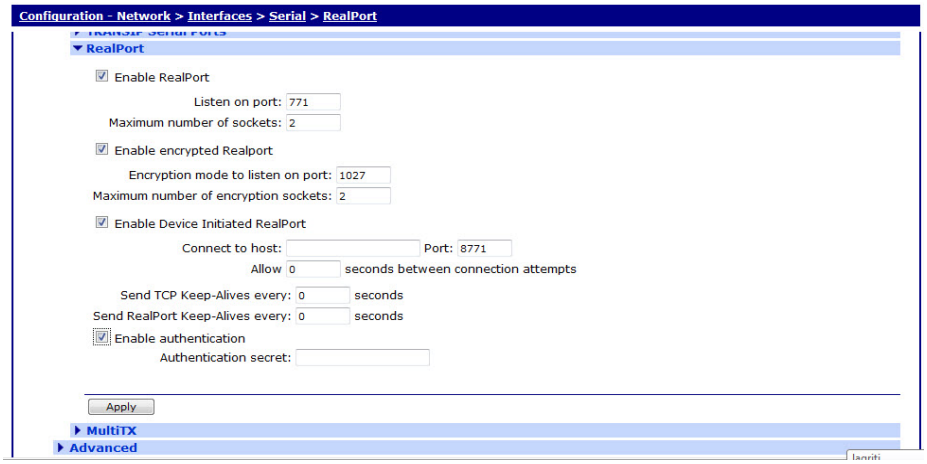
Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
transip	n	port	Valid port number 0 – 65535	Listen on port
transip	n	host	Valid IP address a.b.c.d or hostname	Connect to IPaddress a.b.c.d or Hostname
transip	n	remport	Valid port number 0 – 65535	Port
transip	n	keepact	0 – 255	Send TCP Keep-Alives every s seconds
transip	n	staycon	ON,OFF	Enable Stay Connected mode
transip	n	cmd_echo_off	ON,OFF	Disable command echo
transip	n	escchar	Valid ASCII character	Escape char c
transip	n	esctime	0 – 255	Escape delay s milliseconds

RealPort

Configuration> Network> Serial> Realport

The ***Configuration> Network> Serial> Realport*** page:



Digi devices use the patented RealPort COM/TTY port redirection for Microsoft Windows.

RealPort software provides a virtual connection to serial devices, no matter where they reside on the network. The software is installed directly on the host PC and allows applications to talk to devices across a network as though the devices were directly attached to the host. Actually, the devices are connected to a Digi device somewhere on the network. RealPort is unique among COM port re-directors because it is the only implementation that allows multiple connections to multiple ports over a single TCP/IP connection. Other implementations require a separate TCP/IP connection for each serial port. Unique features also include full hardware and software flow control, as well as tunable latency and throughput. Access to RealPort services can be enabled or disabled.

Encrypted RealPort

Digi devices also support RealPort software with encryption. Encrypted RealPort offers a secure Ethernet connection between the COM or TTY port and a device server or terminal server.

Encryption prevents internal and external snooping of data across the network by encapsulating the TCP/IP packets in a Secure Sockets Layer (SSL) connection and encrypting the data using Advanced Encryption Standard (AES), one of the latest, most efficient security algorithms. Access to Encrypted RealPort services can be enabled or disabled. Digi's RealPort with encryption driver has earned Microsoft's Windows Hardware Quality Lab (WHQL) certification. Drivers are available for a wide range of operating systems, including Microsoft Windows Server 2003, Windows XP, Windows 2000, Windows NT, Windows 98, Windows ME; SCO Open Server; Linux; AIX; Sun Solaris SPARC; Intel; and HP-UX. It is ideal for financial, retail/point-of-sale, government or any application requiring enhanced security to protect sensitive information.

Enable RealPort
Selecting this option enables RealPort on the router.

> **Listen on port**
> This configures the TCP port on which the router will listen for RealPort connections.
>
> **Maximum number of sockets**
> This defines the maximum number of RealPort connections that the router will support.

Enable encrypted RealPort
Selecting this option enables encrypted RealPort on the router.

> **Encryption mode to listen on port**
> This configures the TCP port on which the router will listen for encrypted RealPort connections.
>
> **Maximum number of encryption sockets**
> This defines the maximum number of encrypted RealPort connections that the router will support.

Enable Device Initiated RealPort
Selecting this option enables router to make a RealPort connection to a host PC.

> **Connect to host a.b.c.d Port n**
> This configures the IP address or hostname and TCP port that the router should use when making a device initiated connection.
>
> **Allow s seconds between connection attempts**
> This configures the interval in seconds between device initiated connection attempts.

Send TCP Keep-Alives every s seconds

This configures the interval at which TCP Keep-Alives are sent over the RealPort connection. A value of 0 means that Keep-Alives are not sent.

Send RealPort Keep-Alives every s seconds
This configures the interval at which RealPort Keep-Alives are sent over the RealPort connection. A value of 0 means that Keep-Alives are not sent.

Enable exclusive mode
Selecting this option enables exclusive mode. Exclusive mode allows a single connection from any one RealPort client ID to be connected only. If this setting is enabled and a subsequent connection occurs that has the same source IP as an existing connection, the old existing connection is forcibly reset under the assumption that it is stale.

Enable authentication
Selecting this option enables RealPort authentication.

Authentication secret
This configures the RealPort authentication secret.

Related CLI Commands

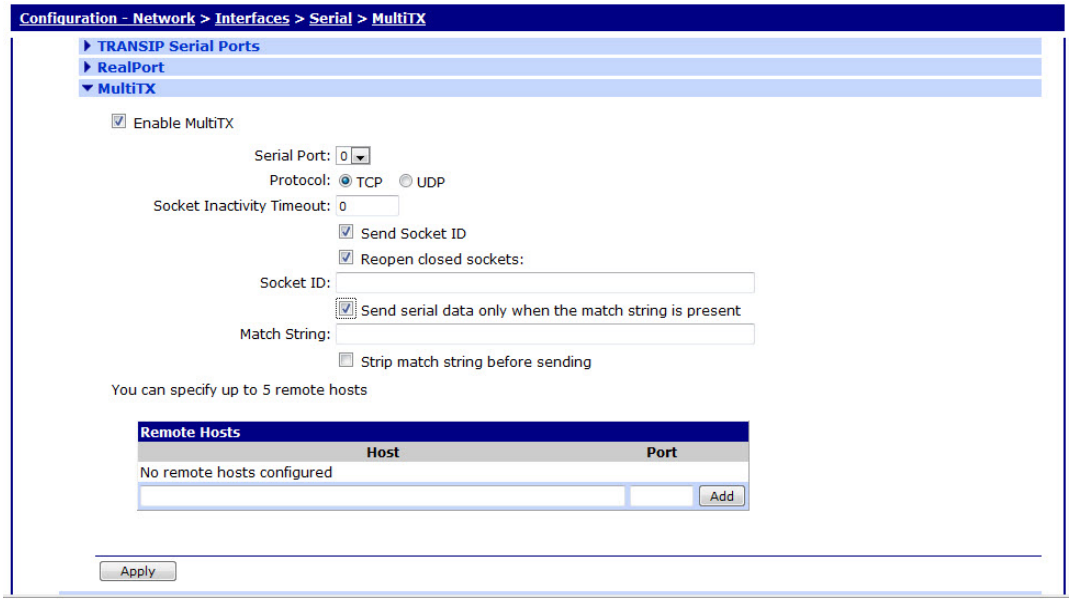
Entity	Instance	Parameter	Values	Equivalent Web Parameter
rport	0	enabled	OFF,ON	Enable RealPort
rport	0	ipport	0 - 65535	Listen on port
rport	0	maxnbsocks	0 - 255	Maximum number of sockets
rport	0	encryption	OFF,ON	Enable encrypted RealPort
rport	0	encport	0 - 65535	Encryption mode to listen on port
rport	0	maxnbencsocks	0 - 255	Maximum number of encryption sockets
rport	0	initiate	OFF,ON	Enable Device Initiated RealPort
rport	0	IPaddr	Valid IP address a.b.c.d	Connect to host a.b.c.d Port n
rport	0	initiateport	0 - 65535	Connect to host a.b.c.d Port n
rport	0	initiatebackoff	0 - 255	Allow s seconds between connection attempts
rport	0	tcpkeepalives	0 - 255	Send TCP Keep-Alives every s seconds
rport	0	rportkeepalives	0 - 255	Send RealPort Keep-Alives every s seconds
rport	0	exclusive	OFF,ON	Enable exclusive mode
rport	0	auth	OFF,ON	Enable authentication
rport	0	secret	Up to 30 characters	Authentication secret
rport	0	status		[Description: displays the current Realport status]
rport	0	trace	0, 1,2,3 0: Off 1: place the	

Entity	Instance	Parameter	Values	Equivalent Web Parameter
			trace information in the analyser trace. 2: print the trace information out of the debug port. 3: place information in the trace	
rport	0	debug	0, 1,2,3 0: Off 1: place the debug information in the analyser trace. 2: printf the debug information out of the debug port. 3: print out the debug port.	
rport	0	dcddiscards	On/Off	[Description: discards data when DCD is OFF from the modem]
rport	0	duplex	0=full 1=half	[description: configures half mode/full duplex modes]

Multitx

Configuration> Network> Serial> MultiTX

The MultiTx page allows users to enable and edit the MultiTx parameters. This supports sending serial data to multiple (up to 5) TCP or UDP destinations. When enabled, the configured ASY port is opened and serial data from the port is sent to all configured destinations.



Enable Multitx
Checking this checkbox displays the MultiTX settings in the GUI and enables the MultiTX function on the router.

Serial Port
This field specifies the serial interface to use. Data received on this serial will be forwarded to all configured remote hosts.

Protocol
This field specifies whether TCP or UDP will be used as the transport method.

Socket Inactivity Timeout

If there is no data transmitted for the specified number of seconds, the socket will be closed. 0 = no timeout.

Send Socket ID
When enabled, the text entered into the 'Socket ID' field is transmitted to the remote host when the socket connects.

Reopen Closed Socket
This enabled an always-on mode. If the socket is closed for any reason, the router will attempt to reconnect to the remote host.

Socket ID
This parameter is used in conjunction with Send Socket ID. Text entered will be transmitted when the socket connects. \r can be used for CR. \n can be used for NL. Hex can be specified by using \xhh where hh is replaced with the hex code, eg \x04 will define binary character 04.

Send serial data only when the match string is present
Match string function is enabled when users check this checkbox.

Match String
When enabled, serial data will only be forwarded to remote hosts when the 'Match String' text is present.

Strip match string before sending

When this parameter is enabled, the text in the 'Match String' field will be removed before the data is forwarded to the remote host.

Remote host
Up to five remote hosts can be specified in these fields.

Host
Enter the hostname or IP address of the remote host in this field.

Port
Enter the TCP or UDP port number that the remote host is listening on.

Add
Click this button to add the remote host.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
multitx	0	enabled	OFF,ON	Enable MultiTx
multitx	0	srcport	OFF,ON (default: OFF)	Serial Port
multitx	0	prot1	OFF,ON (default: OFF)	protocol
multitx	0	send_sockid	0 – 255 (default: 0)	Send Socket ID
multitx	0	keepopen	OFF,ON	Reopen Closed Socket
multitx	0	sockid		Socket ID
multitx	0	fwd_match	0 - 65535	Send serial data only when the match string is present
multitx	0	matchstring	0 - 255	Match String
multitx	0	Strip_match	OFF,ON	Strip match string before sending

Advanced

Configuration – Network > Interfaces > Advanced

The ***Configuration – Network > Interfaces > Advanced*** menu has the following sub-menu options:

- External Modems
- PPP Mappings
- PPP n

Point-to-Point Protocol (PPP) is a standard protocol for transporting data from point to multipoint networks (such as IP) across point-to-point links (such as a serial or ISDN connection). This functionality is essential for dial-up Internet access.

Since data is transferred across IP networks in synchronous format, the router supports asynchronous to synchronous PPP conversion. This allows asynchronous terminals connected to the units to communicate with remote synchronous PPP devices. Normally, this is carried out using a single ISDN B-channel so that data can be transferred at speeds up to 64kbps. This is known as ASYNC to SYNC PPP operation and is supported as standard by most terminal adaptors. To use ASYNC to SYNC PPP operation all that is necessary is to ensure that the PPP protocol is bound to the ASY port to which the terminal or PC is connected. (see ***Configuration – Network > Interfaces > Serial***).

Note:
In order to use ASYNC to SYNC PPP the attached terminal must also support PPP (Windows dial-up networking supports PPP).

In addition to ASYNC to SYNC operation (where the router only converts the PPP from one form to another) the router can initiate its own PPP sessions. This is used for example when:

The router is configured as a router to connect an Ethernet network to the Internet via ISDN or W-WAN

The router is answering an incoming ISDN call with PPP either for remote management or remote access to the Ethernet network to which the router is connected

The router is accessed locally through the serial port for configuration purposes by setting up a Windows Dial-Up-Networking connection to the “phone number” 123

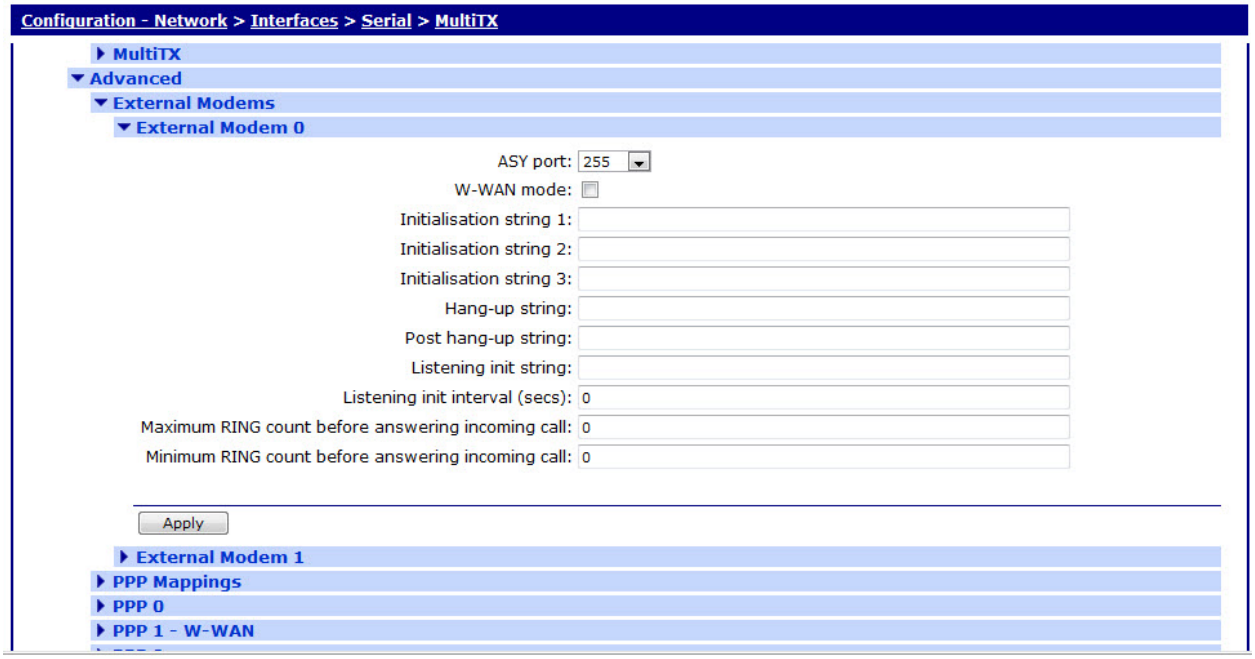
Note:
With the exception of MLPPP the parameters in this section are only relevant when the router is generating the PPP, i.e. they are NOT relevant for ASYNC to SYNC PPP operation.

The unit also supports Multi-link PPP (MLPPP). MLPPP uses both ISDN B-channels simultaneously (and two PPP instances), to provide data transfer speeds up to 128Kbps for applications such as email or establishing a point-to-point connection between two units.

External Modems

Configuration – Network > Interfaces > Advanced> External Modems

The External Modems page contains external modem parameters. External modem support added to GPRS builds. It is now possible to have a GPRS build that can also make outgoing PPP connections via an external modem. It is also possible to answer incoming calls via an external modem. The PPP 'use_modem' field has now been altered so that the value indicates which modem type should be used. Value 1 indicates that GPRS modem should be used, value 2 indicates that external modem should be used.It is now also possible (by including enough modem call control instances) to do multilink PPP over multiple external modems.



ASY Port

This is the physical ASY port for the external modem.

W-WAN mode

Checking the check box enables W-WAN mode

Initialisation string n

These parameters (Initialisation string 1, Initialisation string 2, Initialisation string 3) allow you to specify a number of command strings that are sent to the wireless module each time a wireless connection is attempted. These can be used to set non-standard wireless operating modes.

Each string is prefixed with the characters “AT” before being sent to the wireless module and they are sent to the wireless module in the order specified until an empty string is encountered. For example, Initialisation string 3 will not be sent unless Initialisation string 1 and Initialisation string 2 are both specified. Initialisation strings are not normally required for most applications as the unit will normally be pre-configured for correct operation with most networks.

Hang-up string

In a typical wireless application the connection to the network is “always on” and under normal circumstances it is not necessary to hang-up the wireless module. Under certain circumstances however, the router may use the “ATH” command to try and disconnect the wireless module from the network, e.g. if an incorrect APN has been specified and the module is unable to attach to the network correctly.
This parameter allows you to specify an alternative hang-up string that is sent to the wireless module when disconnecting a call. As with the Initialisation strings, it is not necessary to include the “AT” as this is inserted automatically by the router.

Post hang-up string

This parameter allows you to specify additional “AT” commands that is sent to the wireless module after it has been disconnected. As with the Initialisation strings, it is not necessary to include the “AT” as this is inserted automatically by the router.

Listening init string
This is the listening initialisation string parameter for external modems.

Listening init interval (secs)
The listening init string is sent at intervals specified by a listening init interval parameter.

Maximum RING count before answering incoming call

The count of the maximum number of rings before answering incoming call can be set in this field. The default value is 0.

Minimum RING count before answering incoming call

The count of the minimum number of rings before answering incoming call can be set in this field. The default value is 0.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
modemcc	n	asyport	0 - 255 (Default: 255)	
modemcc	n	init_str	Free text field	Initialisation string 1
modemcc	n	init_str1	Free text field	Initialisation string 2
modemcc	n	init_str2	Free text field	Initialisation string 3
modemcc	n	hang_str	Free text field	Hang-up string
modemcc	n	posthang_str	Free text field	Post Hang-up string
modemcc	0	linit_str	Free text field	Listening init string
modemcc	0	linit_int	0 - 2147483647	Listening init interval (secs)

PPP Mappings

Configuration – Network > Interfaces > Advanced> PPP Mappings

The PPP Mappings page contains two columns of as many interfaces as are supported by the router (this varies between models). Each row in the column contains a drop-down list box that allows the user to select what function should be associated with each PPP instance. The PPP instance number is the left-most column. So, for example, to assign a W-WAN interface to PPP instance 3, select “Mobile SIM1 or SIM2” from the drop-down box to the right of instance “3”. If a W-WAN interface is fitted to the router, this is the default mapping.

Multilink PPP

Configuration – Network > Interfaces > Advanced> PPP Mappings> Multilink PPP

As mentioned above, the routers may support multilink PPP – this section describes the configuration of MLPP functionality.

The PPP interface must be configured with “Always On” mode enabled and an AODI NUA.

Desired local ACCM c

The value in this textbox defines the Asynchronous Control Character Map (ACCM). The default value of 0x00000000 should work in most cases. Changing this value is for advanced users only.

Desired remote ACCM c
The value in this textbox defines the ACCM for the remote peer. As above, the default value of 0xffffffff should work in most cases and should only be changed if it is known that other characters should be used.

Username
The value in this textbox is the username that should be used for logging on to the remote system.

Password
The value in this textbox is the password that should be used for authentication with the remote system when using MLPP. This password is used for both B-channel PPP connections.

Confirm password
When changing the password, the new password should also be typed into this text box. The router will check that both fields are the same before changing the value.

Enable remote CHAP authentication
When checked, this checkbox causes the router to authenticate itself with the remote system using CHAP. If this parameter is set, the connection will fail if authentication fails. Generally, this checkbox should be left unchecked.

Enable short sequence numbers
When checked, this checkbox enables the use of 12-bit, rather than the more usual 16-bit data packet sequence numbers.

Bring up the second ISDN B-channel

Never
When selected, this radio button will cause the router not to activate the second B-channel.

When the data rate is greater than n bytes/sec for s seconds

When this radio button is selected, the two associated textboxes become enabled and allow the user to enter the desired data rate (default 2000 bytes/second) that will trigger activation of the second B-channel and the period for which the data rate exceeds that value, before the channel is activated.

Drop the second ISDN B-channel

When the connection is terminated
When this radio button is selected, the second B-channel is only deactivated when the connection is terminated.

When the data rate is less than n bytes/sec for s seconds
When this radio button is selected, the above two text boxes are enabled. The value in the left-hand one specifies the data rate below which the traffic must fall before the secondary B-channel will be deactivated. The second box contains the time in seconds for which the data rate must be below threshold before the second B-channel is deactivated.

Note:
The following parameters are for use with “Always On Dynamic ISDN”.

Bring up the first ISDN B-channel

When the data rate is greater than n bytes/sec for s seconds

When “Always On” mode is enabled, these two textboxes specify the data rate and duration for which the data rate must be sustained before the B-channel is activated.

Drop the first ISDN B-channel

When the data rate is less than n bytes/sec for s seconds
When “Always On” mode is enabled, these two textboxes specify the data rate below the traffic must fall and the duration for which it is below the threshold before the B-channel is deactivated.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
mlppp	0	l_accm	0x00000000 – 0xFFFFFFFF	Desired local ACCM
mlppp	0	r_accm	0x00000000 – 0xFFFFFFFF	Desired remote ACCM
mlppp	0	username	Valid username	username
mlppp	0	password	Valid password	password
mlppp	0	epassword	Encrypted password	None – this parameter is not configurable
mlppp	0	r_chap	ON, OFF	Enable remote CHAP authentication
mlppp	0	l_shortseq	ON, OFF Default OFF	Enable short sequence numbers
mlppp	0	up_rate	0 – 2147483648 Default 2000	When the data rate is greater than n bytes/sec
mlppp	0	up_delay	0 – 2147483648 Default 10	for s seconds
mlppp	0	down_rate	0 – 2147483648 Default 1000	When data rate is less than n bytes/sec
mlppp	0	down_delay	0 – 2147483648 Default 10	for s seconds
mlppp	0	dup_rate	0 – 2147483648 Default 500	When data rate is greater than n bytes/sec
mlppp	0	dup_delay	0 – 2147483648 Default 5	for s seconds
mlppp	0	ddown_rate	0 – 2147483648 Default 500	When data rate is less than n bytes/sec
mlppp	0	ddown_delay	0 – 2147483648 Default 5	for s seconds

PPP n

Configuration – Network > Interfaces > Advanced> PPPn

This section contains those parameters which may need to be adjusted when setting up a PPP connection but in general can be left at their default values. The ***Configuration – Network > Interfaces > Advanced> PPPn*** submenu has the following sub-menu options:

- Mobile
- Advanced
- PPP Negotiation
- QoS
- Sub-Configs

Load answering defaults
Clicking this button will cause the router to read the default PPP answering default parameters from a default configuration stored in memory.

Load dialling defaults
Clicking this button causes the router to read the PPP dialling parameters from a default configuration stored in memory.

Description
This text box holds a description of the PPP instance that may make it easier to refer to. For example the PPP instance used to connect to an ISP may be named “MyISP”.

This PPP interface will use
If the PPP mappings have been set up previously using the PPP mappings page, this box will contain the name of the protocol that has been assigned to this PPP instance. If the mapping has not been set up previously and if no default mappings apply, the text in the box should read “Not Assigned”. Select the required the required physical interface from the drop-down selection box.

Dial out using numbers
To allow the router to automatically make outgoing calls, the ISDN number must be specified. The four text boxes allow four telephone numbers to be entered. The first one is required, the others are optional and will be used in rotation. These numbers may be the number of the Internet Service Provider (ISP) or another router.

Prefix n to the dial out number
When making outgoing PPP calls, the value specified in this text box is inserted before the actual number being called. This may be required if a PABX system is in use which requires a prefix to be used in order to get an outside line. For example, when using AODI or BACP, the remote peer may provide a number to be used for raising an additional B-channel to increase the bandwidth. However, such a number will not normally include the digits needed to connect to an outside line via a PABX.

Username
The value in this text box is the username to be used for MLPPP login.

Password
This is the password to be used for MLPPP login. This password is used for both B-channel PPP connections.

Confirm password
Type the password in this text box to confirm that the password has been correctly typed in.

Note:

The following three radio buttons control how the IP address for the router is assigned.

Allow the remote device to assign a local IP address to this router

When this radio button is selected, the remote peer will assign this PPP interface an IP address.

Try to negotiate a.b.c.d as the local IP address for this router

If it would be useful, but not essential, to have a predefined IP address for the interface, the second radio button should be selected and the desired IP address entered into the text box to the right.

Use a.b.c.d as the local IP address for this router

If it is essential that the PPP interface has a specific IP address, this radio button should be selected and the IP address entered into the text box.

Use mask a.b.c.d for this interface
The default value in this text box will normally work and should only be changed if it is known that the default is not appropriate. Since PPP is a peer-to-peer protocol this value makes sense in most situations.

Use the following DNS servers if not negotiated

Primary DNS server
The value in this text box is the IP address of the primary DNS server to use if a DNS server is not assigned as part of the PPP negotiation and connection process. It is fairly common practice for the DNS server to be assigned automatically by the ISP when making a connection.

Secondary DNS server
The value in this text box specifies the IP address of the secondary DNS server to use if one is not automatically assigned by the remote peer.

Attempt to assign the following IP configuration to remote devices
When checked, this check box will reveal the following four configuration parameters which control how the PPP instance assigns an IP address to a connecting remote peer. The primary and secondary DNS server addresses will also be sent to the remote peer

Assign remote IP addresses from a.b.c.d to a.b.c.d
The IP addresses in these text boxes define the pool of IP addresses to assign to remote peers during the IP protocol configuration phase of the PPP negotiation process.

Primary DNS server
The value in this text box is the IP address of the primary DNS server that the remote peer should use when making DNS requests over the link.

Secondary DNS server
The value in this text box is the IP address of the secondary DNS server that the remote peer should use when making DNS requests, should the primary server be unavailable.

Allow the PPP interface to answer incoming calls
When checked, this checkbox will cause the PPP instance to answer an incoming call.

Only allow calling numbers ending with n
When set to answer calls, the value in this textbox provides a filter for ISDN sub-addresses. This value is blank by default but when the PPP instance is set to answer calls, only numbers having trailing digits that match the sub-address value in this test will be answered. So for example, if this value is set to “123”, only calls from numbers with trailing digits that match this value will be answered. For example 01942 605123

Close the PPP connection after s seconds
The value in this textbox specifies the maximum time that the link will remain active in any one session. After this time, the link will be deactivated.

if it has been up for m minutes in a day
The router will deactivate the PPP instance after it has been active for the value specified in this text box.

if it has been idle for h hrs m mins s secs
The router will deactivate the PPP instance after the time specified in these text boxes if it detects that the link has not seen traffic.

Alternative idle timer for static routes s seconds
The value in this text box specifies an alternative inactivity timeout for use in conjunction with the "Make PPP n interface use the alternative idle timeout when this route becomes available" parameter on the ***Configuration – Network > IP Routing/Forwarding > Static Routes > Routes n > Advanced*** web page. This timeout will only be used until the PPP instance next deactivates. After that the normal timeout value is used.

If the link has not received any packets for s seconds
The value in this text box specifies the amount of time that the router will wait without receiving any PPP packets before disconnecting. The timer is reset with each received PPP packet.

if the negotiation is not complete in s seconds
The value in this textbox specifies the maximum time (in seconds) allowed for the PPP negotiation to complete. If negotiations have not completed within this period, the interface is deactivated.

Enable NAT on this interface
When checked, this checkbox causes the router to apply Network Address Translation (NAT) to IP packets on this interface. When enabled, the following additional parameters appear:

IP address/IP address and Port
These radio buttons select whether IP address translation only should be applied or whether port number translation should also be applied to IP packets.

NAT Source IP address a.b.c.d
This text box contains the IP address of the interface that should be used as the source address in IP packets crossing the NAT interface.

Enable IPsec on this interface
When checked, this checkbox causes the router to use the IPsec protocol to secure the connection. When enabled, the following additional parameters appear:

Keep Security Associations (SAs) when this PSTN interface is disconnected
When checked, this checkbox causes the router to maintain (i.e. not flush) the SA when the interface becomes disconnected. The normal behaviour is to remove the SAs when the interface becomes disconnected.

Use interface x,y for the source IP address of IPsec packets
If it is required to use another interface (i.e. not the interface currently being configured) as the source address for IPsec packets, this may be achieved by selecting the desired interface from the drop-down list and typing the desired interface instance number into the adjacent text box.

Enable the firewall on this interface
Checking this checkbox causes the router to apply the firewall settings to traffic using this interface. When debugging connections issues it is often helpful to ensure that this checkbox

is NOT checked, as incorrect firewall rules will prevent a connection from passing network traffic. If the connection works when the firewall is turned off but fails when turned on, a good place to start checking parameters would be in the firewall settings page, ***Configuration – Security > Firewall***.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	name	Free text field	Description
ppp	n	phonenum	up to 25 digits	Dial out using numbers
ppp	n	ph2	"	"
ppp	n	ph3	"	"
ppp	n	ph4	"	"
ppp	n	prefix	0 – 9999999999	Prefix n to the dial out number
ppp	n	username	Valid username	Username
ppp	n	password	Valid password	Password
ppp	n	epassword	The encrypted password	None – this parameter is not configurable
ppp	n	IPaddr	Default 0.0.0.0 set automatically	Allow the remote device to assign a local IP address to this router
ppp	n	IPaddr	Valid IP address a.b.c.d	Try to negotiate a.b.c.d as the local IP address for this router
ppp	n	IPaddr	Valid IP address Default 1.2.3.4	Use a.b.c.d as the local IP address for this router
ppp	n	mask	Valid IP address Default 255.255.255.255	use mask a.b.c.d for this interface
ppp	n	DNSserver	Valid IP address	Primary DNS server
ppp	n	secDNS	Valid IP address	Secondary DNS server
ppp	n	DNSport	Valid IP address Default 53	DNS Port
ppp	n	IPmin	Valid IP address Default 10.10.10.10	Assign remote IP addresses from a.b.c.d to a.b.c.d
ppp	n	IPrange	0 – 255 Default 5	Assign remote IP addresses from a.b.c.d to a.b.c.d Note that these are not directly equivalent. This address is obtained by adding the range value to the minimum.
ppp	n	transDNS	Valid IP address	Primary DNS server
ppp	n	sectransDNS	Valid IP address	Secondary DNS server

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	cingnb	up to 25 digits	Only allow numbers ending with n
ppp	n	msn	up to 9 digits	with ISDN MSN ending with n
ppp	n	sub	up to 17 digits	with ISDN sub-address ending with n
ppp	n	maxup	0 – 2147483648	Close the PPP connection after s seconds
ppp	n	maxuptime	0 – 2147483647	if it has been up for m minutes in a day
ppp	n	timeout	Default 300s (5 minutes)	if it has been idle for h, m, s
ppp	n	timeout2	0 – 2147483648	Alternative idle timer for static routes s seconds
ppp	n	rxtimeout	0 – 2147483648	if the link has not received any packets for s seconds
ppp	n	maxneg	0 – 2147483648	if the negotiation is not complete in s seconds
ppp	n	do_nat	0,1 0 = Off 1 = On	Enable NAT on this interface
ppp	n	natip	Valid IP address a.b.c.d	NAT Source IP address a.b.c.d
ppp	n	ipsec	0,1 0 = Off 1 = On	Enable IPsec on this interface
ppp	n	ipsecent	Default PPP Ethernet	Use interface x,y for the source address of IPsec packets
ppp	n	ipsecadd	Valid interface number	Use interface x,y for the source address of IPsec packets
ppp	n	firewall	OFF, ON	Enable the firewall on this interface

Mobile

Configuration – Network > Interfaces > Advanced>PPP n> Mobile

Mobile telephone modules fitted into the router use PPP to connect to the network and send and receive traffic. This section describes parameters relevant to setting up a mobile telephone module.

Use SIM Any, SIM1, SIM2
These radio buttons are used to select which of the SIM cards fitted should be used by the module.

Detach W-WAN if the link fails
When checked, this checkbox will cause the router to issue the command to detach the mobile telephone module from the wireless network if it detects that the link has failed. Link failure is detected by a PPP ping response timer or by a firewall request.

Detach W-WAN between connection attempts
This checkbox controls whether or not the module stays attached to the network if multiple connection attempts are required to establish a connection. This functionality may be useful if the connection to the mobile telephone network is not very reliable. Connecting to the mobile telephone network to send and receive data is a two-stage process. The first stage is where the module signals its wish to join the network and is accepted by the local cell. The second stage involves negotiating the link parameters and transferring data. Sometimes it may be necessary to cleanly detach from the network in order to start the process from the ground up.

Related CLI commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	gprs_sim	0 – 2 0 = Any 1 = SIM1 2 = SIM2	Use SIM, Any, SIM 1, SIM 2
ppp	n	detach_on_fail	OFF,ON	Detach W-WAN if the link fails
ppp	n	detach	OFF,ON	Detach W-WAN between connection attempts

Advanced

Configuration – Network > Interfaces > Advanced> PPP n> Advanced

This section contains PPP configuration parameters that do not normally need changing from the defaults and are therefore placed in a separate section to reduce clutter on the web pages.

Metric
This parameter specifies the connected metric of the interface. The default metric of a connected interface is 1. By allowing the interface to have a higher value (lower priority), static routes can take precedence over interfaces. For normal operation, leave the value in this textbox unchanged.

Allow this PP interface to settle for s x 100 milliseconds
On wireless links it is possible that the initial packets sent to the interface by the TCP layer may be dropped by the network if they are sent too quickly after PPP negotiation has completed. The value in this textbox defines the delay in notification sent to the TCP layer that PPP negotiation has completed.

Enable “Always On” mode of this interface
If the “always on” option is available on the interface, checking this checkbox reveals the following two radio buttons. When this functionality is enabled, the router will automatically try to reconnect after about 10 seconds if the link becomes disconnected. This parameter should be enabled when using AODI or W-WAN.

On
Default action, the interface will always try and raise this PPP link.

On and return to service immediately

These two radio buttons enable the “always-on” functionality and additionally the facility to return to the in-service state after a disconnect event.

Put this interface “Out of Service” when an always-on connection attempt fails
Normally, always-on interfaces will not go out of service unless they have connected at least once. When checked, this checkbox causes the router to put the interface out of service even if the first connection attempt fails.

Attempt to re-connect after s seconds
The parameter in this textbox specifies the length of time in seconds that the router should wait after an “always-on” PPP connection has been terminated before trying to re-establish the link.

If a PPP interface that would be inhibited by this PPP is connected, attempt reconnection after s seconds
The value in this textbox takes precedence over the previous parameter when another PPP instance that is usually inhibited by this one is connected. This parameter would typically be used to reduce the connection retry rate when a lower priority PPP instance is connected.

Wait s seconds after power-up before activating this interface
The value in this textbox is the initial delay that the router will apply before activating the PPP instance after power-up. After the initial power-up delay the normal always-on activation timers apply. If set to zero, no delay will be applied.

Keep this interface up for at least s seconds
The value in this textbox specifies the minimum period that the PPP interface should remain available. This means that even if the link becomes inactive before this period expires, the connection will remain open.

Enable Multilink PPP on this interface
When checked, this checkbox enables the multilink PPP capability of the router. (See above for configuration details).

Click here to assign a timeband to this interface
Clicking this link redirects the browser to the timeband configuration page ***Configuration – Network > Timebands***.

Add a route to a.b.c.d if the peer’s IP address is not negotiated
Normally, the IP address for a device connecting to a remote peer is assigned by the remote peer. If this is not the case then the router will need a route to the remote peer. The value in this textbox is set to the IP address of the remote peer so that it can be added to the routing table.

Forward IP broadcasts over this interface if the interface is on the same IP network as an Ethernet interface
When checked, this checkbox causes the router to route broadcast packets to and from Ethernet interfaces. This will only occur if the PPP instance has issued an address which is part of the Ethernet interface network.

Send LCP echo request packet to the remote peer
When checked, this checkbox reveal the configuration parameters that cause the router to send Link Control Protocol (LCP) packets to the remote peer at specified intervals. This facility can be useful for keeping a link active (W-WAN, for example).

Send LCP echo requests every s seconds
The value in this text box sets the interval at which to send the packets. When set to zero, the transmission of LCP packets is disabled.

Disconnect the link after n failed echo requests
The value in this text box set the number of consecutive failed echo requests that are allowed before the router terminates the link. When set to zero, this functionality is disabled, i.e. the router will not terminate the link if the LCP echo requests do not elicit a response from the remote.

Generate Heartbeats on this interface
When checked, this checkbox reveals the configuration options that control how the router sends heartbeat packets. Generating a valid configuration enables the router to send heartbeat packets to the specified destination. Heartbeat packets are UDP packets that contain various items of information about the router and which may include status information that may be used to locate its current dynamic IP address. Heartbeats may also contain GPS position information and mobile telephone module information.

Send Heartbeat messages to IP address a.b.c.d every h hrs, m minutes, s secs
The left-hand text box contains the IP address of the destination for the heartbeat packets. The remaining text boxes specify the desired interval between sending heartbeat packets.

Use interface x,y for the source IP address
These two text boxes allow selection of the source interface for the UDP heartbeats. Selecting an Ethernet source will allow the packets to follow the routing table instead of being sent out from the PPP interface on which they are set.

Select transmit interface using the routing table
When checked, this checkbox causes the router to choose the best route from the routing table. If unchecked, the exit interface will be the interface on which the heartbeat is configured.

Include IMSI information in the Heartbeat message
When checked, this checkbox causes the router to include the IMSI of the wireless MODEM module in the heartbeat packet.

Include GPS information in the Heartbeat message
When checked, this checkbox causes the router to include the GPS co-ordinates in the heartbeat packet.

Generate Ping packets on this interface
When checked, this checkbox causes the router to reveal the configuration parameters that enable the sending of ICMP echo request (ping) packets. This feature can be used as part of a backup interface strategy.

Send n byte pings to IP host a.b.c.d every h hrs, m mins, s secs
These parameters control how the ICMP echo requests are generated. The value in the left-hand text box specifies the number of data bytes in the echo request. Typical values are 32 or 64 octets. The IP host text box specifies the IP address of the host to which the ping packets are sent. The remaining parameters specify how often the ping should be sent.

Send pings every h hrs, m mins, s seconds if ping responses are not being received
These three text boxes specify the interval at which to send pings when more than one ping request is outstanding. When left at the default of zero this function is disabled.

Switch to sending pings to IP host a.b.c.d after n failures
These parameters allow for more reliable problem detection before failover occurs. If the value in the first text box is a valid IP address, and the value in the second text box is greater than zero, when a ping failure is detected on the primary host address, this

secondary host is tried. This is to ensure that should the primary host become unavailable for any reason and stops responding to the ICMP echo requests, the router will check an alternative IP address before initiating the failover procedure. The value in the second text box is the number of pings that should be allowed to fail before checking the secondary IP address.

Ping responses are expected within s seconds
When the value in this text box is set to a non-zero value, the router will wait for that specified interval for a response from a ping request before applying the timeout specified in the "**Send pings every ... if ping responses are not being received**" setting above. If the value is set to 0 (the default) then the router applies the timeout without modification.

Only send Pings when this interface is "In Service"
When checked, this checkbox causes the router to only send ICMP requests when the PPP instance is in service. The default setting is unchecked which means that ICMP requests are sent when the interface is in service and out of service.

New connections to resume with previous Ping interval
When checked, this checkbox causes the router to use the ping interval that was in force when the PPP interface last disconnected.

Reset the link if no response is received within s seconds
The value in this text box specifies the period for which the router should wait before terminating the PPP connection if no response to the auto-pings has been received. This behaviour is useful in the attempt to re-establish communications, since the router will automatically attempt to restart an always-on link that has been terminated. This function is primarily used where IP traffic is being carried over a W-WAN link and where the associated PPP instance has been configured into the always-on mode.

Use ETH 0 IP address as the source IP address
When checked, this checkbox causes the router to use the IP address of interface ETH 0 as the source address for ICMP echo requests instead of the current IP address of the PPP interface.

Defer sending pings if IP traffic is being received
One of the uses for sending ICMP echo requests is as a keepalive mechanism. When this checkbox is checked, it causes the router to defer sending the ping packets out if IP traffic is being received, since in this case, separate keepalives are not needed.

Limit the data transmitted over this interface
Some service providers impose a (usually monthly) limit on the amount of data sent over a link and levy additional charges if the limit is exceeded. This is fairly common practice for W-WAN links. When checked, this checkbox causes the router to stop sending data on the interface when the preset data limit has been exceeded. The interface is unlocked manually by clicking the "**Clear Total Data Transferred**" button on the ***Management – Network Status > Interfaces > Advanced > PPP > PPP n*** page. Alternatively, it may be reset automatically on a certain day of the month – see below.

Issue a warning event after n Kbytes/Mbytes/GBytes
The value in this text box is the amount of traffic which will cause a warning event to be generated in the event log stating that the specified amount of data has been transferred. The units are specified by a drop-down list, having the following options; KBytes, MBytes, GBytes. For example, if the monthly tariff includes up to 5MB of data before excess useage charges are levied, it would be useful to set this threshold to 4MB. This would cause the router to create a warning entry in the event log once 4MB of data

had been transferred. This event could then be used to trigger an email alert, SNMP trap or SMS alert message.

Stop data from being transmitted after n Kbytes/Mbytes/GBytes
The value in this text box specifies the total amount of data that may be transmitted by this PPP instance before the link is blocked for further traffic, and the value in the drop-down list specifies the units which are; KBytes, MBytes, GBytes.

Reset the data limit on the n day of the month
The value in this text box defined the day of the month on which the data limit is reset to zero.

Reset this interface if n packets are transmitted and the connection has been up for at least s seconds
The values in these text boxes control the circumstances under which the link may be reset. If the number of packets text box has a value greater than zero, the router will reset the link if that many IP packets have been transmitted but none have been received, and the link has been active for at least the value specified in the second text box.

Reboot the router after n consecutive resets
If the value in this text box is non-zero, the router will reboot if the PPP link has been reset the specified number of times as a consequence of the value n packets (described immediately above) being exceeded.

Reboot the router after n consecutive connection failures
If the value in this text box is non-zero, the router will reboot if it fails to establish a connection over this PPP instance after the specified number of consecutive attempts.

Allow this PPP interface to attempt to connect n times before allowing other PPP interfaces inhibited by this interface to connect
The value in this textbox specifies the number of connection attempts this PPP instance is allowed to make before other PPP instances that are inhibited by this instance may make connection attempts.

If this PPP interface gets disconnected, allow it to attempt to reconnect n times before allowing other PPP interfaces inhibited by this interface to connect
On W-WAN routers, the value in this textbox specifies the number of times that a PPP instance which was connected and is then disconnected, is allowed to attempt to reconnect before other PPP instances that were inhibited by this PPP instance will be allowed to connect.

Inhibit this PPP interface if the following PPP instances n are Active | Active and not out of service | Not out of service | Connected and not out of service
Inhibition of this PPP interface may be controlled by the state of other PPP instances. This behaviour is controlled by the options in this drop-down menu box.

If this PPP interface is inhibited and data needs to be sent
The options in this drop-down selection box control the behaviour of the router in the situation where the PPP instance is in its inhibited state but there is data waiting to be sent over the interface. The options are:

Do not bring up interface
This option leaves the situation as it is with the interface remaining inhibited.

Bring up interface and use normal idle period
This option removes the inhibit state from the interface and uses the normal idle time associated with it to control when it deactivates.

Bring up interface and use idle period of s seconds

This option causes the interface to become activated but rather than using the idle timer associated with the interface, specify the idle timeout.

Inhibit other PPP interface if this PPP interface is disconnected but operational
When checked, this checkbox enables this PPP instance to inhibit other PPP instances if it is operational but not currently active.

Attempt to negotiate DEFLATE compression on this interface
When checked, this checkbox causes the router to compress the data transferred over this link. When unchecked, compression is disabled. The effectiveness of data compression will vary with the type of data but a typical ratio achieved for a mix of data such as web pages, spreadsheets, databases, text files and (uncompressed) image files would be between 2:1 and 3:1. Using compression has the effect of increasing the effective throughput. Using compression may offer cost savings on a network where charges are based upon the amount of data transferred (e.g. W-WAN networks). If the data is already compressed (e.g. .zip files or JPEG images) then the compression algorithm will detect this and send the data without attempting further compression.

Attempt to negotiate MPPE encryption on this interface
When checked, this checkbox causes the router to attempt to negotiate Microsoft Point-to-Point Encryption (MPPE) with the remote peer. If the remote peer is unable to negotiate MPPE, negotiations will fail. When negotiated, the PPP instance will encrypt the PPP frames as per the MPPE specification.

MPPE key size
The values in this drop-down list select the length (in bits) of the encryption key. The options are:

- Auto
- 40 bits
- 56 bits
- 128 bits.

"Auto" indicates that the router will accept whatever the remote suggests. For the other values, the remote must accept and request the key size specified, else the PPP negotiations will fail.

Enable MPPE stateless mode
When this checkbox is checked, the router will negotiate stateless mode in which the session key is changed after the transmission of each packet. Stateless mode may be useful for lossy links.

Note:
MPPE does not provide authentication, only encryption. This is because the encryption keys are determined by the PPP engines themselves on start-up.

TCP transmit buffer size n bytes
When the value in this text box is set to a non-zero value, the router will use the value to set the size of the TCP buffer for transmitted packets. This is useful for slow and/or lossy connections such as satellite links. Setting this buffer to a low value will prevent the amount of unacknowledged data from getting too high. If retransmits are required, a smaller TX buffer helps prevent retransmits flooding the connection.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	metric	0 - 255	Metric

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	settledly	0 - 200	Allow this PPP interface to settle for s seconds after the connection has come up
ppp	n	aodion	0 – 2 0 = disabled 1 = enabled 2 = On and return to service immediately	Enable “Always On” mode of this interface, On, On and return to service immediately
ppp	n	immoos	ON, OFF	Put this interface “Out of Service” when an always-on connection attempt fails
ppp	n	aodi_dly	0 – 2147483647	Attempt to reconnect after s seconds
ppp	n	aodi_dly2	0 – 2147483647	If a PPP interface that would be inhibited by this PPP is connected, attempt to re-connect after s seconds
ppp	n	pwr_dly	0 - 2147483647	Wait s seconds after power-up before activating this interface
ppp	n	minup	0 - 2147483647	Keep this interface up for at least s seconds
ppp	n	multi	OFF, ON	Enable Multilink PPP on this interface
ppp	n	netip	Valid IP address a.b.c.d	Add a route to a.b.c.d if the peer’s IP address is not negotiated
ppp	n	rbcast	OFF, ON	Forward IP broadcasts over this interface if this interface is on the same IP network as an Ethernet interface
ppp	n	echo	0 - 2147483648	Send LCP echo requests every s seconds
ppp	n	echodropcnt	0 - 2147483648	Disconnect the link after n failed echo requests
ppp	n	hrtbeatip	Valid IP address a.b.c.d	Send Heartbeat messages to IP address a.b.c.d every h hrs, m mins, s secs
ppp	n	hrtbeatint	0 - 2147483648	Send Heartbeat messages to IP address a.b.c.d every h hrs, m mins, s secs
ppp	n	hbipent	Blank, PPP, ETH Blank is default	Use interface x,y for the source IP address

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	hbipadd	Valid interface number 0 - 2147483648	Use interface x,y for the source IP address
ppp	n	hbiproute	OFF, ON	Select transmit interface using the routing table
ppp	n	hbimsi	OFF, ON	Include IMSI information in the Heartbeat message
ppp	n	hbgps	OFF, ON	Include GPS information in the Heartbeat message
ppp	n	pingsiz	0 - 2147483648	Send n byte ping to IP host a.b.c.d every h hrs, m mins, s secs
ppp	n	pingip	Valid IP address a.b.c.d	Send n byte ping to IP host a.b.c.d every h hrs, m mins, s secs
ppp	n	pingint	0 - 2147483648	Send n byte ping to IP host a.b.c.d every h hrs, m mins, s secs
ppp	n	pingint2	0 - 2147483648	Send pings every h hrs, m mins, s seconds if ping responses are not being received
ppp	n	pingip2	Valid IP address a.b.c.d	Switch to sending pings to IP host a.b.c.d after n failures
ppp	n	ip2count	0 - 2147483648	Switch to sending pings to IP host a.b.c.d after n failures
ppp	n	pingresp	0 - 2147483648	Ping responses are expected within s seconds
ppp	n	pingis	OFF, ON	Only send Pings when this interface is “In Service”
ppp	n	ping2cont	OFF, ON	New connections to resume with previous Ping interval
ppp	n	pingdeact	0 - 2147483648	Reset the link if no response is received within s seconds
ppp	n	pingfreth0	OFF, ON	Use ETH 0 IP address as the source IP address
ppp	n	pingresetint	OFF, ON	Defer sending pings if IP traffic is being received
ppp	n	dlwarnkb	0 - 2147483647	Issue a warning event after n XBytes
ppp	n	dlstopkb	0 - 2147483647	Stop Data from being transmitted after n XBytes

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	dlrstday	0 – 255	Reset the data limit on the n day of the month
ppp	n	sscnt	0 - 2147483648	Reset this interface if n packets are transmitted and the connection has been up for at least s seconds
ppp	n	sssecs	0 - 2147483648	Reset this interface if n packets are transmitted and the connection has been up for at least s seconds
ppp	n	lscnt	0 - 2147483648	Reboot the router after n consecutive resets
ppp	n	rebootfails	0 - 2147483648	Reboot the router after n consecutive connection failures
ppp	n	acttries	0 - 255	Allow this PPP interface to attempt to connect n times before allowing other PPP interfaces inhibited by this interface to connect
ppp	n	pdacttries	0 - 255	If this PPP interface gets disconnected, allow it to attempt to reconnect n times before allowing other PPP interfaces inhibited by this interface to connect
ppp	n	inhibitno	0 - 2147483648	Inhibit this PPP interface if the following PPP instances n are Active, Active and not out of service, not out of service, Connected and not out of service
ppp	n	inhmode	0 - 3	Inhibit this PPP interface if the following PPP instances n are Active, Active and not out of service, not out of service, Connected and not out of service
ppp	n	actmode	OFF,ON	Inhibit other PPP interface if this PPP is interface is disconnected but operational
ppp	n	trafficto	0 - 2147483648	If this PPP interface is inhibited and data needs to be sent do not bring up the interface, bring up interface and use normal idle period, bring up interface and use idle period of

Entity	Instance	Parameter	Values	Equivalent Web Parameter
				s seconds
ppp	n	deflate	0,1 0 = Off 1 = On	Attempt to negotiate DEFLATE compression on this interface
ppp	n	mppebits	0, 40, 56, 128 0 = Auto	MPPE key size
ppp	n	mppeless	OFF, ON	Enable MPPE stateless mode
ppp	n	tcptxbuf	0 - 2147483648	TCP transmit buffer size n bytes

PPP Negotiation

Configuration – Network > Interfaces > Advanced> PPP n> PPP Negotiation

When PPP starts up, the devices at both ends of the link negotiate the link parameters, in order to find a common subset that both devices can use. The negotiation may be summarized by saying that both ends send negotiation packets that say “these are the values that I wish to use and these are the values that I wish you to use”

Restrict the negotiation time to s seconds
The parameter in this text entry box specifies the maximum time allowed for a PPP negotiation to complete. If negotiations have not completed in this time, the PPP instance is disconnected.

Desired local ACCM
The value in this text box is the local Asynchronous Control Character Map which has the default value 0x00000000. Changing this value is for advanced users.

Desired remote ACCM
This text box holds the remote ACCM which has the default value 0xffffffff. As above, the default will work in nearly all circumstances and should be changed only where really necessary.

Desired local MRU n bytes
The value in this text box is the desired local Maximum Receive Unit (MRU), the default value of 1500 octets will work fine in most cases.

Desired remote MRU n bytes
The value in this text box is the desired MRU for the remote end of the link. The default value of 1500 octets will be fine in most cases.

Request local ACFC
When checked, this checkbox causes the router to request Address Control Field Compression (ACFC). When negotiated, the address/control fields are removed from the start of the PPP header.

Request remote ACFC
When checked, this checkbox causes the router to ask the remote device to request ACFC.

Request local PAP authentication
When checked, this checkbox causes the router to use the Password Authentication Protocol (PAP) before allowing a connection to be made. Generally, this parameter is enabled for incoming connections and disabled for outgoing connections.

Request remote PAP authentication

When checked, this checkbox causes the router to authenticate itself with the remote device using PAP. If this parameter is set, the connection will fail if authentication is not successful. Generally, this parameter is disabled.

Request local CHAP authentication
When checked, this checkbox causes the router to use the Challenge Handshake Authentication Protocol (CHAP) for local authentication. As with PAP, this parameter is generally enabled for incoming connections and disabled for outgoing connections.

Request remote CHAP authentication
As with PAP above, this checkbox controls whether or not the router should authenticate itself with the remote device using CHAP. The connection will fail if authentication fails. Generally, this parameter is enabled for outgoing connection and disabled for inbound connections.

Request local (VJ) compression
When checked, this checkbox causes the router to request the use of Van Jacobson compression which compresses TCP/IP headers to about 3 rather than the standard 40 octets. This is generally only used to improve efficiency on slow links.

Request remote (VJ) compression
When checked, this checkbox causes the router to send a negotiation packet that requests that the remote device requests VJ compression.

Request local PFC
When checked, this checkbox causes the router to request Protocol Field Compression (PFC) which compresses PPP protocol fields from 2 to 1 octet.

Request remote PFC
When checked, this checkbox causes the router to ask the remote device to request Protocol Field Compression.

Request BACP
When this checkbox is checked, the router will use the Bandwidth Allocation Control Protocol (BACP) to determine the ISDN number to dial for the seconds or third multi-link connection.

Request callback
When checked, this checkbox will request a callback when it dials into a remote device. Note that the answering PPP instance of the remote unit must also be configured with the telephone number of the calling unit and a suitable username, password combination.

Allow remote end to request callback
This drop-down list controls whether or not the router will respond to incoming callback requests. The options are:

- Off
- Desired
- Required.

Allow this unit to authenticate using

CHAP-MD5
Selecting enabled from the drop-down menu will allow the router to authenticate logins using the CHAP MD-5 algorithm.

MS-CHAP
Selecting enabled from the drop-down menu will allow the router to authenticate logins using Microsoft's proprietary MS-CHAP algorithm.

MS-CHAPv2

Selecting enabled from the drop-down menu will allow the router to authenticate logins using version 2 of Microsoft's proprietary MS-CHAP algorithm.

Allow a remote unit to authenticate using

CHAP-MD5
When checked, this checkbox will allow the router to authenticate with a remote unit using the CHAP-MD5 algorithm.

MS-CHAP
When checked, this checkbox will allow the router to authenticate with a remote unit using Microsoft's MS-CHAP algorithm.

MS-CHAPv2
When checked, this checkbox will allow the router to authenticate with a remote unit using version 2 of Microsoft's MS-CHAP algorithm.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	maxneg	0 - 2147483648	Restrict the negotiation time to s seconds
ppp	n	l_accm	0x00000000 – 0xFFFFFFFF Default 0x00000000	Desired local ACCM
ppp	n	r_accm	0x00000000 – 0xFFFFFFFF Default 0xFFFFFFFF	Desired remote ACCM
ppp	n	l_mru	0 – n Default 1500	Desired local MRU
ppp	n	r_mru	0 – n Default 1500	Desired remote MRU
ppp	n	l_acfc	OFF, ON	Request local ACFC
ppp	n	r_acfc	OFF, ON	Request remote ACFC
ppp	n	l_pap	OFF, ON	Request local PAP authentication
ppp	n	r_pap	OFF, ON	Request remote PAP authentication
ppp	n	l_chap	OFF, ON	Request local CHAP authentication
ppp	n	r_chap	OFF, ON	Request remote CHAP authentication
ppp	n	l_comp	OFF, ON	Request local (VJ) compression
ppp	n	r_comp	OFF, ON	Request remote (VJ) compression
ppp	n	l_pfc	OFF, ON	Request local PFC
ppp	n	r_pfc	OFF, ON	Request remote PFC

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	l_bacp	OFF, ON	Request BACP
ppp	n	l_callb	OFF, ON	Request callback
ppp	n	r_callb	0 – 2 0 = Off 1 = Desired 2 = Required	Allow remote end to request callback
ppp	n	l_md5	0 - 2 0 = Disabled 1 = Enabled 2 = Preferred	Allow this unit to authenticate using CHAP-MD5
ppp	n	r_md5	0,1 0 = Off 1 = On	Allow remote unit to authenticate using CHAP-MD5
ppp	n	l_ms1	0,1 0 = Disabled 1 = Enabled 2 = Preferred	Allow this unit to authenticate using MS-CHAP
ppp	n	r_ms1	0,1 0 = On 1 = Off	Allow remote unit to authenticate using MS-CHAP
ppp	n	l_ms2	0 - 2 0 = Disabled 1 = Enabled 2 = Preferred	Allow this unit to authenticate using MS-CHAPv2
ppp	n	r_ms2	0,1 0 = Off 1 = On	Allow remote unit to authenticate using MS-CHAPv2

QoS

Configuration – Network > Interfaces > Advanced> PPPn> QoS

The parameters on this page control the Quality of Service management facility. Each PPP instance has an associated QoS instance, where PPP 0 maps to QoS 0, PPP 1 maps to QoS 1 and so on. These QoS instances include ten QoS queues into which packets may be placed when using QoS. Each of these queues must be assigned a queue profile from the twelve available.

Enable QoS on this interface
This checkbox, when checked, reveals the following QoS configuration parameters:-

Link speed n Kbps
The value in this text entry box should be set to the maximum data rate that this PPP link is capable of sustaining. This is used when calculating whether or not the data rate from a queue may exceed its minimum Kbps setting as determined by the profile assigned to it and send at a higher rate (up to the maximum Kbps setting).

Queue n

Below this column heading, is a list of ten queue instances. Each instance is associated with the profile and priority on the same row.

Profile n
This column contains the profile to be associated with the queue. There are twelve available, 0 – 11, which are selected from the drop-down list boxes.

Priority
This column contains drop-down menu boxes which are used to assign a priority to the selected queue. The priorities available are: “Very High”, “High”, “Medium”, “Low”, and “Very Low”.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
qos	n	linkkbps	0 -	Link speed n kbps
qos	n	q0prof	0 - 11	Queue 0 Profile
qos	n	q0prio	0 – 4 0 = Very high 1 = High 2 = Medium 3 = Low 4 = Very Low	Queue 0 Priority
qos	n	q1prof	0 – 11	Queue 1 Profile
qos	n	q1prio	0 – 4	Queue 1 Priority
qos	n	q2prof	0 - 11	Queue 2 Profile
qos	n	q2prio	0 – 4	Queue 2 Priority
qos	n	q3prof	0 - 11	Queue 3 Profile
qos	n	q3prio	0 – 4	Queue 3 Priority
qos	n	q4prof	0 - 11	Queue 4 Profile
qos	n	q4prio	0 – 4	Queue 4 Priority
qos	n	q5prof	0 - 11	Queue 5 Profile
qos	n	q5prio	0 – 4	Queue 5 Priority
qos	n	q6prof	0 - 11	Queue 6 Profile
qos	n	q6prio	0 – 4	Queue 6 Priority
qos	n	q7prof	0 - 11	Queue 7 Profile
qos	n	q7prio	0 – 4	Queue 7 Priority
qos	n	q8prof	0 - 11	Queue 8 Profile
qos	n	q8prio	0 – 4	Queue 8 Priority
qos	n	q9prof	0 - 11	Queue 9 Profile
qos	n	q9prio	0 – 4	Queue 9 Priority

Sub-Configs

Configuration – Network > Interfaces > Advanced> PPP n > Sub-Configs

PPP sub-configs can be used as an alternative to using an entire PPP instance if only a few parameters are different to those in an existing PPP instance. Using PPP sub-configs saves on system memory. Up to 50 sub-configs may be defined.

Nb
This is the instance number for a sub-config.

Description
The text in this text box is used as a name to easily identify the sub-config.

Username
The value in this text box is the username that should be used when authenticating with the remote system and is usually only required for outgoing PPP calls.

Password
The value in this text box is the password used for authentication with the remote system.

Confirm
When changing the password, it should be entered into this text box also to allow the router to check for simple typing errors.

Dialout Number
The value in this text box is the ISDN number used to make outgoing calls. This must be a valid number in order to allow the router to make outgoing calls. This number could be the number of the Internet Service Provider (ISP) or another router.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
pppcfg	1 - 50	name	Up to 25 characters	Description
pppcfg	1 - 50	username	Valid username up to 60 characters	Username
pppcfg	1 - 50	password	Valid password up to 40 cahracters	Password
pppcfg	1 - 50	phonenum	Up to 25 digits	Dialout Number

DHCP Server

Configuration – Network > DHCP Server

Digi routers incorporate one or more Dynamic Host Configuration Protocol (DHCP) servers, one for each Ethernet port. DHCP is a standard internet protocol that allows a DHCP server to dynamically distribute IP addressing and configuration information to network clients.

This section contains a web page (***Configuration – Network > DHCP Server***) for each of the DHCP servers. Additionally, there is a separate page for mapping MAC addresses to fixed IP addresses. The ***Configuration – Network > DHCP Server*** menu has the following sub-menu options:

- DHCP Server for Ethernet n

- Logical Ethernet Interfaces
- DHCP Options
- Static Lease Reservations

DHCP Server for Ethernet n

Configuration – Network > DHCP Server> DHCP Server for Ethernet n

Enable DHCP Server
When checked, this checkbox opens up the page to reveal the following parameters:

IP Addresses a.b.c.d to a.b.c.d
There are six text boxes in this part of the page; three rows of two. The values in these specify the starting and ending addresses for the range of IP addresses that will be handed out by the DHCP server. Each of the three rows can be used to specify a different IP address pool, all pools should be within the same subnet. When the minimum IP address text box is clear, the DHCP service will be disabled. In other words, in order to enable the DHCP service, there must be at least one minimum IP address and a range.
Using the CLI, this is specified slightly differently, a starting address and a range are specified instead.

Mask
The value in this text box specifies the subnet mask used to on the network to which the router is connected.

Gateway
A gateway is required in order to route data to IP addresses that are not on the local subnet. The value in this text box specifies the IP address of the gateway (which is usually the IP address of the router itself as configured by the IP address of the Ethernet interface associated with this DHCP instance). Alternatively, this may be set to the IP address of another router on the LAN.

DNS Server
The value in this text box specifies the IP address of the primary DNS server to be used by clients on the LAN. This will usually be the IP address of the route itself. Alternatively, this may be set to the IP address of an alternative DNS server on the LAN.

Secondary DNS Server
The value in this text box specifies the IP address of a secondary DNS server (if available) to be used by DHCP clients on the LAN.

Domain Name
The value in this text box specifies the domain name which will be returned to clients.

Lease Duration d days h hrs m mins
The values in these three text boxes specify how long a DHCP client may use the assigned IP address before it must renew its configuration with the DHCP server. When configuring this value using the command line interface be aware that this parameter is specified in minutes. The three boxes here are for convenience when using long lease durations.

Wait for s milliseconds before sending DHCP offer reply
When the checkbox box is checked, the router will use the value in the text box as the delay to use prior to sending out the DHCP_OFFER message. Enabling this functionality and setting the delay to a non-zero value will allow other DHCP servers on the network to respond first.

Only send offers to Wi-Fi clients

When checked, this checkbox causes the router to only send DHCP offers to Wi-Fi clients. This is useful if the router is being used as an access point and there is a separate DHCP server on the Ethernet LAN.

DHCP Relay

Forward DHCP requests to a.b.c.d
The values in these two text boxes specify the IP addresses of the two supported DHCP relay agents. If the DHCP server is on a different subnet, specifying the IP address of the server in this text box will cause the router to forward DHCP requests to the IP address specified. The DHCP server must be within 4 hops.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dhcp	n	IPmin	Valid IP address a.b.c.d	IP Addresses a.b.c.d
dhcp	n	IPrange	0 – 2147483647 Default 20	to a.b.c.d
dhcp	n	IPmin2	Valid IP address a.b.c.d	IP Addresses a.b.c.d
dhcp	n	IPrange2	0 – 2147483647 Default 0	to a.b.c.d
dhcp	n	IPmin3	Valid IP address a.b.c.d	IP Addresses a.b.c.d
dhcp	n	IPrange3	0 – 2147483647 Default 0	to a.b.c.d
dhcp	n	mask	Valid IP address a.b.c.d	Mask
dhcp	n	gateway	Valid IP address a.b.c.d	Gateway
dhcp	n	DNS	Valid IP address a.b.c.d	DNS Server
dhcp	n	DNS2	Valid IP address a.b.c.d	Secondary DNS Server
dhcp	n	domain	Up to 64 characters	Domain Name
dhcp	n	lease	0 – 2147483648 minutes Default 20160 minutes (14 days)	Lease Duration d days, h hrs, m mins
dhcp	n	respdelms	0 - 2147483647	Wait for s milliseconds before sending DHCP offer reply
dhcp	n	wifionly	Off,On	Only send offers to Wi-Fi clients
dhcp	n	fwdip	Valid IP address a.b.c.d	Forward DHCP requests to a.b.c.d

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dhcp	n	fwdip2	Valid IP address a.b.c.d	Forward DHCP requests to a.b.c.d

Advanced

Configuration – Network > DHCP Server> *DHCP Server for Ethernet n> Advanced*

Next Bootstrap Server a.b.c.d
The value in this text box specifies the IP address of a secondary configuration server. This server does not have to be on the same logical subnet as the client.

Server Hostname
The value in this text box specifies the name of a host that the DHCP client can make contact with in order to download a boot file.

Boot file
The value in this text box specifies the name of the boot file the client can download from the host specified in the Server Hostname text box.

Send unicast responses
This parameter is used to send unicast responses rather than broadcast responses.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dhcp	n	nxtsvr	Valid IP address a.b.c.d	Next Bootstrap Server
dhcp	n	sname	Up to 64 characters	Server Hostname
dhcp	n	file	Up to 64 characters	Boot file
dhcp	n	unicasttx	Off,On	Send unicast responses

Advanced DHCP Options

Configuration – Network > DHCP Server> DHCP Server for Ethernet n> Advanced DHCP Options

NetBIOS Name Server a.b.c.d
The value in this text box specifies the IP address of the primary WINS server address.

Secondary NetBIOS Name Server a.b.c.d
The value in this text box specifies the IP address of the secondary WINS server address.

TFTP Server Address a.b.c.d
The value in this text box specifies the IP address of a TFTP server. This is mainly used for boot images.

FTP Server Address a.b.c.d (for WYSE Terminals)
The value in this text box specifies the IP address of an FTP server and is a custom option for use with WYSE terminals.

FTP Root Dir (for WYSE Terminals)
The value in this text box specifies the root directory for FTP transfers. This is also a custom option for use with WYSE terminals.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dhcp	n	NBNS	Valid IP address a.b.c.d	NetBIOS Name Server a.b.c.d
dhcp	n	NBNS2	Valid IP address a.b.c.d	Secondary NetBIOS Name Server a.b.c.d
dhcp	n	tftp	Valid IP address a.b.c.d	TFTP Server Address a.b.c.d
dhcp	n	ftp	Valid IP address a.b.c.d	FTP Server Address a.b.c.d
dhcp	n	ftproot	Up to 64 characters	FTP Root Dir

Logical Ethernet Interfaces

Configuration – Network > DHCP Server> Logical Ethernet Interfaces

The web pages in this section are simply a duplicate of the above pages but applying to logical, rather than physical Ethernet interfaces.

DHCP Options

Configuration – Network > DHCP Server> DHCP Options

The DHCP Option pages allow custom (or non-standard) DHCP options to be configured and sent to the DHCP client when requesting an IP address and other DHCP parameters. This is useful for devices such as IP telephones that use specific strings. On the web page, these (up to ten) options are configured using a table. The table contains the following fields:

Option
The value in this box specifies the DHCP option number.

Data type
The value in this text box specifies the data type for the option and can be any one of the following; 1,2 or 4 byte value, IPv4 address, text string or hexadecimal data.

Value
The value in this text box specifies the actual data that will be sent in the DHCP option message.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dhcpopt	n	optnb	0 - 2147483647 Default 0	Option
dhcpopt	n	type	i1 = 1 byte value i2 = 2 byte value	Data type

Entity	Instance	Parameter	Values	Equivalent Web Parameter
			i4 = 4 byte value ipv4 = IPv4 address string = string hex = hexadecimal	
dhcpopt	n	value	Up to 127 octets	Value

Command line examples

To set the option number to "9" for LPR Server, the command is:

dhcpopt 0 optnb 9

Static Lease Reservations

Configuration – Network > DHCP Server> Static Lease Reservation

The table on this web page controls the configuration of MAC address to IP address mappings and is used to assign a specific IP address to a particular Ethernet MAC address. This is particularly useful for mobile applications, e.g. W-WAN where a particular item of mobile equipment should be issued with the same IP address regardless of when it was last connected to the network. Up to ten MAC to IP address reservations may be specified.

Note:
It is important to ensure that the IP addresses specified her DO NOT fall within the IP address ranges specified in the DHCP server page.

IP Address a.b.c.d
The value in this box specifies the IP address to be assigned.

MAC Address aa.bb.cc.dd.ee.ff
The value in this box specifies the MAC address which is to be given the above IP address.

As is usual with the configuration tables, clicking the **Add** button adds the entry to the table and clicking the **Delete** button removes an existing entry from the table.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
mac2ip	n	IPaddr	Valid IP address a.b.c.d	IP Address a.b.c.d
mac2ip	n	mac	Valid MAC address aa.bb.cc.dd.ee.ff	MAC Address aa.bb.cc.dd.ee.ff

Two separate commands are required to set up a mapping, these are:

mac2ip <instance> mac <MAC address>

mac2ip <instance> IPaddr <IP address>

where <*instance*> can be 0 – 9.

Network Services

Configuration – Network > Network Services

The web page described here collects together a number of services that are provided by the router into one section to enable the user to quickly enable or disable these services without having to navigate to multiple sections of the menu. Detailed configuration is performed within the specific section.

Enable Network Management Protocol (SNMP)
Click on this checkbox to enable and disable remote management of the router using SNMP. This checkbox does not actually directly control the SNMP functionality, but enables or disables the remaining SNMP controls on this page.

Note:
Simply clicking on this checkbox may not be sufficient to allow this service to start working. Depending upon the version selected below, additional configuration may be required.

Detailed configuration, including setting up command filters, users and SNMP traps are to be found at ***Configuration > Remote Management > SNMP***

Enable SNMP v1
When this checkbox is checked, the router will use version 1 of the protocol.

UDP Port n
The standard UDP port that is used by this service is 161 which is used as the default. If a different port is required, enter the port number into the text entry box.

Enable SNMP v2c
When this checkbox is checked, the router will use version 2c of the protocol.

Enable SNMP v3
When this checkbox is checked, the router will use version 3 of the protocol.

Enable Simple Network Timer Server (SNTP)
When checked, the router will act as an SNTP time server.

Source
This drop-down selection menu selects the source used to supply time data for the SNTP server. The usual options are:

- internal real time clock (RTC) device
- a GPS module (if supported)
- an NTP client (if supported).

Enable Secure Shell Server (SSH / SFTP)
The simplest way to check the status or configuration of the router or to upload new firmware is to use the CLI over a directly connected ASY port or via a telnet session. Both of these options have security implications. If a user wishes to gain access to the command line interface of the router but using a more secure protocol, then selecting this checkbox will enable a secure shell to start. This option also enables support for SFTP for secure file transfers.

Enable Telnet Server
This radio button selects between a simple telnet server or telnet over SSL. When this option is selected, the simple, insecure version of telnet is enabled.

Enable Telnet over SSL
If security is an issue, then selecting this option with the radio button disables the simple version and enables telnet over the secure socket layer (SSL) protocol.

Enable Web Server (HTTP)
Much of the configuration of the router may be performed using the web GUI as described here. However, HTTP is an insecure protocol and so for security reasons, this service may be disabled by deselecting this radio button and hence, enabling the following secure web

server. If security is not such an issue, selecting this option allows the simpler and slightly more convenient web server to be used.

Enable Secure Web Server (HTTPS)
Select this radio button to disable the insecure HTTP protocol and enable the HTTPS service.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snmp	n	v1enable	0,1 0 = Off 1 = On	Enable SNMP v1
snmp	n	port	Default 161	UDP Port n
snmp	n	v2cenable	0,1 0 = Off 1 = On	Enable SNMP v2c
snmp	n	v3enable	0,1 0 = Off 1 = On	Enable SNMP v3
sntp	0	srvr_mode	ON,OFF	Enable Simple Network Time Server (SNTP)
sntp	0	time_src	0 = RTC 1 = GPS 2 = NTP Client	Source
sockopt	n	ssh_server_ena	ON, OFF	Enable Secure Shell Server
sockopt	n	telnets	ON, OFF	Enable Telnet over SSL
sockopt	n	https	ON, OFF	Enable Secure Web Server

DNS Servers

Configuration – Network > DNS Servers

This section describes the parameters used to configure the DNS server functionality of the router. The ***Configuration – Network > DNS*** menu has the following sub-menu options:

- DNS Server n
- DNS Server Update

DNS Server n

Configuration – Network > DNS Servers> DNS Server n

The DNS server selection parameters give the ability to specify a DNS server based on the DNS query. For example, DNS lookups for internal servers can be directed to an internal DNS server and all other DNS requests can be sent direct to an external DNS server managed by the ISP.

For DNS requests matching pattern, send the request to
This text box contains the hostname pattern to match for the specified DNS server. This parameter needs a wildcard to prefix the domain name. For example, to match DNS queries for all digi.com servers, enter *.digi.com.

When using this feature, it is recommended that the last DNS server selection hostname pattern is set to "*" to match all other DNS lookups. This ensures that all the DNS lookup configuration is kept together for ease of troubleshooting. If this is not done, the lookups will use the DNS server configured on the interface of the default route.

DNS Server a.b.c.d
The value in this text box specifies the IP address of the DNS server to use when a DNS request matches the hostname pattern.

Secondary DNS Server a.b.c.d
In the event of the primary DNS server not being available, the IP address in this text box specifies the destination for DNS queries matching the hostname pattern.

Route using

Routing table / Interface x,y
The two radio buttons associated with this text control whether the router should look up the route to the DNS server by using the routing table or should send the DNS query out of a specific interface. When the Interface radio button is selected, the drop-down box and interface instance text box are enabled. The options available for the interface are PPP and Ethernet. The adjacent text box should be filled in with the number of a valid instance of the interface, e.g. Ethernet 3. (Different models of router support different numbers of interfaces).

Use source IP Address of

Sending interface / Interface x,y
The two radio buttons control whether the DNS query should go out having the source address of the sending interface or a different interface. This will be required for routing if the route to the DNS server is via an IPsec tunnel, to ensure the local and remote subnet selectors match.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dnssel	n	pattern	*.domain.com	For DNS requests matching pattern, send the request to
dnssel	n	svr	Valid IP address	DNS Server a.b.c.d
dnssel	n	secsvr	Valid IP address	Secondary DNS Server a.b.c.d
dnssel	n	ent	PPP,Ethernet	Interface x,y
dnssel	n	add	Valid interface number	Interface x,y
dnssel	n	ipent	PPP,Ethernet	Interface x,y
dnssel	n	ipadd	Valid interface number	Interface x,y

DNS Server Update

Configuration – Network > DNS Servers> DNS Server Update

“Dynamic DNS” is supported in accordance with RFC2136 and RFC2485. This allows units to update specified DNS servers with their IP addresses when they first connect to the Internet and at regular intervals thereafter. The parameters in this section control how the router updates a specified DNS server with its IP address when it first connects to the Internet and at regular intervals thereafter.

This is not to be confused with the popular dynamic DNS service dyndns.com, there is a separate page for configuring the router to work with dyndns.com

Send an update to DNS Server a.b.c.d for
The IP address in this text box specifies the DNS server that should be sent the updated information. The server must support “DNS Update messages”. Dynamic DNS is generally offered as a subscription-based service by ISPs, but for a large number of deployed routers, it may be more appropriate to set up a dedicated DNS server locally.

Name
The value in this text box specifies the member of the DNS zone to update. This name is used in conjunction with the zone parameter (below) to uniquely identify the router. So, for example, if the router has a name of “epos33”, the full address of the unit will be “epos33.mycompany.com”.

Zone
The value in this text box specifies the DNS zone to update. When using Dynamic DNS it will be necessary to have domain name (this may be purchased from an appropriate vendor). This domain name, e.g. “mycompany.com” is what should be entered into the zone field.

When the default route changes

Interface x,y becomes active

The two radio buttons determine when the update is sent, i.e. when the default route changes or when the specified interface becomes active. The drop-down list offers the options of “PPP” or “Ethernet” and the text box is used to enter the instance number for the specified interface.

Also send an update every h hrs, m mins, s secs
The values in these text boxes specify the interval at which the unit will issue update messages to the DNS server.

The DNS server should delete all previous records
When checked, this checkbox causes the DNS server to delete all records of previous addresses served to the unit.

DNS Server Username
The value in this text box is the username that has been allocated by the Dynamic DNS service provider.

DNS Server Password
The value in this text box is the password that has been allocated by the Dynamic DNS service provider.

Password is Base64 encoded
Some Dynamic DNS servers issue passwords that are Base64 encoded, e.g. Linux Base servers. If this is the case, check this check box to switch on the Base64 decoding of the password before transmission. The password is not actually transmitted as part of the message but is used to create a “signature” that is appended to the message. If the password is issued as a hexadecimal string and not straight text, the password in the password text box must be given the prefix “0x”.

Confirm DNS Server Password
The password should be entered into this text box to confirm it.

Local time offset from GMT

Auto detect
The two radio buttons here control whether or not the offset of the local time from GMT should be auto-detected or specified. This feature is required since a GMT timestamp must be included as part of the authentication message. When set to auto-detect the router will automatically apply the correction. When auto detect is not selected, the correct offset should be selected from the drop-down list.

Required Time Accuracy
The value in this text box specifies the permitted variance between the router's time and that of the DNS server. If the time difference exceeds this limit, the DNS update will fail.

Allow DNS clients to cache this entry for s seconds
The value in this text box specifies how long a router that resolved the address is allowed to cache that address for.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dnsupd	0	server	Valid IP address a.b.c.d	Send an update to DNS Server a.b.c.d
dnsupd	0	name	up to 20 characters	Name
dnsupd	0	zone	up to 64 characters	Zone
dnsupd	0	ifent	PPP,ETH	when interface x,y becomes active
dnsupd	0	ifadd	Valid instance number	when interface x,y becomes active
dnsupd	0	upd_int	0 – 2147483648 (seconds)	Also send an update every h hrs, m mins s secs
dnsupd	0	delprevrr	OFF,ON	The DNS server should delete all previous records
dnsupd	0	username	Valid username (up to 20 characters)	DNS Server Username
dnsupd	0	password	Valid password (up to100 characters)	DNS Server Password
dnsupd	0	b64pwd	OFF,ON	Password is Base64 encoded
dnsupd	0	autozone	OFF,ON	Local time offset from GMT auto detect

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dnsupd	0	tzone	–2147483648 - 2147483647 (hours)	Local time offset from GMT n
dnsupd	0	fudge	0 – 2157483648 (seconds)	Required Time Accuracy s seconds
dnsupd	0	ttl	0 – 2157483648 (seconds)	Allow DNS clients to cache this entry for s seconds

Dynamic DNS

Configuration – Network > Dynamic DNS

The Dynamic DNS client (DynDNS) is used to update DNS hostnames with the current IP address of a particular interface. It operates in accordance with the specification supplied by dyndns.com (go to http://www.dyndns.com/developers/specs/). When the interface specified by the interface and interface instance number parameters connects, the client checks the current IP address of that interface and if it differs from that obtained from the previous connection, www.dyndns.com is contacted and the hostnames specified in the Hostname parameters are updated with the new address.

Service Provider
This parameter is used to specify the Dynamic DNS service that will be updated with the router's IP address. Although the protocol is standard, there are subtle differences in the implementation. Choose Dynamic DNS for services provided by dyn.com. Choose No-IP for services provided by noip.com. Choose **Other** for any other service using the Dynamic DNS standard.

Service Provider Hostname
When selecting 'Other' as the service provider, this text field should be used to specify the provider name. This text will be added to the HTTP update string sent to the remote server. The service provider hostname should be obtained by contacting the service provider's own technical support.

Host and Domain Name(s)
These five text boxes specify up to five host/domain names that are to be updated using the service.

Destination port #
The value in this text box specifies the IP port to use as the destination port. The default value is 0 which causes the router to use the default port number which is port 80.

DynDNS User Name
The value in this text box specifies the username to use when updating the hostnames. This will have been supplied by the service provider.

DynDNS Password
The value in this text box specifies the password to use when updating the hostnames. This will have been supplied by the service provider.

Confirm DynDNS Password
Enter the password into this text box to confirm it.

DynDNS DDNS System

The value selected from this drop-down list is used to identify the dynamic DNS system containing the hostnames to be updated. The available options are:

- Dynamic DNS
- Static DNS
- Custom DNS.

When default route/interface x,y becomes active, send DDNS update

The radio buttons select whether or not the router should use the default interface or the interface specified from the drop-down list. If the specified interface option is selected, the required interface is selected from the drop-down list and the interface instance is entered into the adjacent text box. If the default interface is selected, the client will keep track of and use the current default route.

Use Wildcards

This drop-down list selects whether or not wildcard matching on the hostname will be performed. The options are:

- Disable wildcards
- Enable wildcards
- No change to service settings.

When enabled, the Dynamic DNS service will match DNS requests of the form "*.hostname" where "*" matches any text. For example, if Hostname1 was set to "site.dyndns.com" and wildcard matching was enabled, than www.site.dyndns.com would resolve to the interface address.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dyndns	0	provider	dyndns, noip, other	Service provider
dyndns	0	provider_provider	Up to 40 characters	Service Provider Hostname
dyndns	0	hostname1	Up to 40 characters	Host and Domain Name(s)
dyndns	0	hostname2	Up to 40 characters	Host and Domain Name(s)
dyndns	0	hostname3	Up to 40 characters	Host and Domain Name(s)
dyndns	0	hostname4	Up to 40 characters	Host and Domain Name(s)
dyndns	0	hostname5	Up to 40 characters	Host and Domain Name(s)
dyndns	0	port	0 - 65535	Destination port #
dyndns	0	username	Up to 20 characters	DynDNS User Name
dyndns	0	password	Up to 25 characters	DynDNS Password
dyndns	0	system	Blank, statdns, custom	DynDNS DDNS System

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dyndns	0	ifent	Blank,ETH,PPP	When default route/interface x,y becomes active, send DDNS update
dyndns	0	ifadd	0 -2147483647	When default route/interface x,y becomes active, send DDNS update
dyndns	0	wildcard	0,1,2 0 = Disable wildcards 1 = Enable wildcards 2 = No change to service settings	Use Wildcards
dyndns	0	provider_hostname	Up to 40 characters	[Decription: User specified service provider]

Advanced

Configuration – Network > Dynamic DNS> Advanced

The parameters in this section do not normally need changing from their defaults.

Update interval d days
The value in this text box specifies the number of days between dynamic DNS updates.

Supply the IP address in the update
When checked (the default), this checkbox cause the router to supply the IP address as part of the dynamic DNS update. When unchecked, the IP address is not supplied and the DYNDNS server attempts to determine the correct IP address by other means (IP source address in update packet). This mode would normally only be used if the router is behind a NAT router.

Note:
It may be helpful to visit the www.dyndns.com website before attempting configuration of dynamic DNS.

Only send update when this router is the VRRP master
When checked, this checkbox causes the router NOT to send DDNS updates unless at least one Ethernet interface is a VRRP master.

Enable debug
When checked, this checkbox enables debug tracing of the dynamic DNS transactions.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dyndns	0	updateint	0 -255	Update interval d days
dyndns	0	noip	OFF,ON	Supply the IP address in the update
dyndns	0	ifvrrpmaster	OFF,ON	Only send update when this router is the VRRP master

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dyndns	0	debug	OFF,ON	Enable debug

IP Routing / Forwarding - An introduction to TransPort routing

Configuration – Network > IP Routing/Forwarding

The ***Configuration – Network > IP Routing/Forwarding*** menu has the following sub-menu options:

- IP Routing
- Static Routes
- RIP
- OSPF
- BGP
- IP Port Forwarding / Static NAT Mappings
- Multicast Routes

The TransPort's routing table can be viewed by navigating to ***Management - Network Status > IP Routing Table.***

The TransPort's routing table can also be displayed using the CLI command:

`route print`

Types of route

TransPort routers support three main types of route:

Dynamic Routes

Static Routes

Default Routes

Dynamic Routes

Dynamic routes are created automatically when an interface is configured or connected.

For example configuring an Ethernet 0 interface with an IP address of 192.168.1.1 and mask of 255.255.255.0 will cause a dynamic route to be created automatically.

Thus any packet with destination IP address in the range 192.168.1.0 to 192.168.1.255 will automatically be routed through to the Ethernet 0 interface.

Static Routes

Static routes can be added by configuring a route in ***Configuration - Network > IP Routing/Forwarding > Static Routes > Routes 0 – 9 > Route n*** (where n is an instance number).

The minimum configuration required to add a static route is:

IP Address

Mask

Interface

Interface number

If a static route is “pointing” at an Ethernet interface then optionally a gateway IP address can be added. If a gateway IP address is not added then the gateway IP address configured for the Ethernet interface itself will be used automatically.

Default Routes

Default routes can be added by configuring a route in ***Configuration - Network > IP Routing/Forwarding > Static Routes > Default Route n*** (where n is an instance number).

Default routes will match packets with any destination IP address (when in service).

If a default route is configured, packets with destination IP addresses that do not match any of the dynamic or static routes will be sent out the interface specified in the first “in service” default route.

Routing modes

The TransPort has 2 routing modes available, these are:

TransPort routing mode

This is the original routing method and may be seen on existing installations.

CIDR routing mode

Now enabled by default on new TransPort routers.

The CLI command to switch between the 2 modes is:

ip 0 cidr [off|on]

TransPort routing mode

CIDR routing is disabled

When the TransPort receives an IP packet to route, the routing table is used to decide through which interface to send the packet.

Usually the destination IP address of the IP packet is compared with the IP Address and Mask of each entry in the routing table in index order regardless of the order in the routing table or length of mask.

There may be more than one match and in this case the index number of the route is taken into account. The index number is simply the route number in the config, Static Route 0 or 1 is index 0 or 1

Static routes are checked first, then dynamic routes, then default routes.

CLI command: *ip 0 cidr off*

CIDR routing mode

CIDR routing is enabled

When the TransPort receives an IP packet to route, the routing table is used to decide through which interface to send the packet.

Usually the destination IP address of the IP packet is compared with the IP Address and Mask of each entry in the routing table.

There may be more than one match and in this case the most specific route is used to route the packet. Ie, a matching /24 route is used before a matching /16 route.

If multiple routes match the destination and have the same prefix length, the index number of the routes in the routing table is used to determine the route.

CLI command: *ip 0 cidr on*

Route Metrics

Route Metric settings can be set to override the order in which the routes are searched.

Routes with lower metric numbers will always be used in preference to routes with higher metric numbers even if the routes with higher metric numbers appear first in the routing table.

Route metrics can be configured by means of the route parameters:

Connected Metric

Disconnected Metric

Route metrics can be altered automatically according to various circumstances. This is in order to provide automatic backup connection paths.

Routes and interfaces can be put out of service.

Whenever an interface is out of service (oos) any route pointing at the interface will also be out of service.

Whenever a route is out of service, the metric value will be set to 16 in TransPort routing mode and 17 in CIDR mode.

IP Routing

Configuration – Network > IP Routing/Forwarding> IP Routing

Enable CIDR routing
When this checkbox is checked, the following six text boxes are revealed:

Connected Interfaces
The value in this text box specifies the CIDR metric that the router should apply to connected interfaces.

Static Routes
The value in this text box is the CIDR metric that the router should use for static routes. (Default 1)

eBGP Routes
The value in this text box is the CIDR metric that the router should use for eBGP routes. (Default 20).

OSPF Routes
The value in this text box is the CIDR metric that the router should use for OSPF routes. (Default 110)

RIP Routes
The value in this text box is the CIDR metric that the router should use for RIP routing. (Default 120).

iBGP Routes
The value in this text box is the CIDR metric that thae router should use for iBGP routes. (Default 200).

Maximum static route metric

The value in this text box defines the maximum value for the routing metric. The default value is 16.

Route directed IP broadcasts
When checked, this checkbox causes the router to route directed broadcasts. The default state for this parameter is “Off”. A directed broadcast is an IP packet with a destination address that is a valid broadcast address for a subnet but does not originate from that subnet. Directed IP broadcasts are used to send a broadcast from one interface to the subnet of another.

Wait s seconds before using an alternative route
The value in this text box specifies the latency to apply before passing traffic on an alternative route in the current route becomes unavailable.

If an interface is configured for “dial on demand” and fails to connect,

Mark a static route as “Out Of Service” for s seconds
The value in this text box specifies the default time that a route should be marked as out of service if the interface it uses fails to establish a connection.

When an “Always On” route becomes “In Service”, wait s seconds before using it
The value in this text box specifies the delay that the router should apply to a route before passing traffic on it once it has come into service.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ip	0	cidr	on,off	Enable CIDR routing
ip	0	admin_connected	0 - 2147483647	Connected Interfaces
ip	0	admin_static	0 - 2147483647	Static Routes
ip	0	admin_ebgp	0 - 2147483647	eBGP Routes
ip	0	admin_ospf	0 - 2147483647	OSPF Routes
ip	0	admin_rip	0 - 2147483647	RIP Routes
ip	0	admin_ibgp	0 - 2147483647	iBGP Routes
ip	0	inf_metric	0 - 2147483647	Maximum static route metric
ip	0	route_dbcast	0 - 255	Route directed IP broadcasts
ip	0	route_dly	0 - 2147483647	Wait s seconds before using an alternative route
ip	0	route_dwn	0 - 2147483647	If an interface is configured for “dial on demand” and fails to connect, Mark a static route as “Out Of Service” for s seconds

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ip	0	routeup_dly	0 - 2147483647	When an “Always On” route becomes “In Service”, wait s seconds before using it

Static Routes

Configuration – Network > IP Routing/Forwarding> Static Routes

The static routing web pages and command line parameters described below control the static routing table used by the router. These allow the setting up of static IP routes for particular IP subnets, networks or addresses.

Route n

Configuration – Network > IP Routing/Forwarding> Static Routes> Route n

Each of the static route instances has its own configuration page. These are described below:

Description
The value in this text box is to allow a memorable name for the route to be assigned.

Destination Network a.b.c.d
The value in this text box is the IP address of the destination subnet, network or IP address for the route. If the router receives a packet with a destination IP address that matches the Destination Network/Mask combination it will route the packet through the interface specified below.

Mask a.b.c.d
The value in this text box is the network mask that is used in conjunction with the above destination network address to specify the.

Gateway a.b.c.d
The value in this text box is used to override the default gateway IP address configured for the Ethernet interfaces. Packets matching the route will use the gateway address specified in the route rather than the address specified on the Ethernet interface configuration page. This parameter does NOT apply to routes using PPP interfaces.

Interface x,y
The interface used to route the packets is selected from the drop-down list and the interface instance number is entered into the adjacent text box. The available options are:

- None
- PPP
- Ethernet
- Tunnel

Use PPP sub-configuration
If PPP sub-configs are defined, this text will appear in normal highlighting (i.e. not “greyed out”) and text box will accept the number for the desired sub-config to use on this route. This parameter will not appear at all on those models which do not support PPP sub-configurations.

Metric n
The value in this text box is the routing metric to use when the interface is connected. This should have a value between 1 and 16 and is used to select which route should be used when the subnet for a packet matches more than one of the IP route entries.

Each route may be assigned a “connected metric” and a “disconnected metric”. The connected metric parameter is used to specify the metric for a route whose interface is active. The disconnected metric is used to specify the metric for a route whose interface is inactive. Normally both values should be the same but in some advanced routing scenarios necessary to use different values.
If a particular route fails it will automatically have its metric set to 16 which means that it is temporarily deemed as being “out of service”. The default out of service period is set by the IP route out of service parameter on the .... page. Note however, that this default period may be overwritten in certain situations such as when a firewall stateful inspection rule specifies a different period. When a route is out of service, any alternative routes (with matching subnets) will be used first.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
route	n	descr	Up to 20 characters	Description
route	n	IPaddr	Valid IP address a.b.c.d	Destination Network a.b.c.d
route	n	mask	Valid netmask a.b.c.d	Mask a.b.c.d
route	n	gateway	Valid IP address a.b.c.d	Gateway
route	n	ll_ent	Blank,PPP,ETH,TUN	Interface x,y
route	n	ll_add	0 – 2147483647	Interface x,y
route	n	upmetric	0 – 2147483647	Metric

Advanced

Configuration – Network > IP Routing/Forwarding> Static Routes> Route n> Advanced

Use metric n when the interface is not active
The value in this text box specifies the routing metric to use when the interface is not active.

Use this route only if the source IP address of the packet matches
When this checkbox is checked, the following two parameters are enabled.

IP Address a.b.c.d
If necessary, these IP Address and Mask parameters may be used to further qualify the way in which the router routes packets. If the values in this text box and the following Mask parameter are set, the source address of the packet being routed must match these parameters before the packet will be routed through the specified interface.

Mask a.b.c.d
The value in this text box specifies the netmask that is used in conjunction with the IP address as explained above.

Include this route in RIP advertisements
When checked, this checkbox will cause the router to include this static route to be included in RIP advertisements.

Make PPP n interface use the alternative idle timeout when this route becomes available
When checked, this check box, in conjunction with the PPP interface instance number in the text box will cause the router to use the alternative inactivity timeout specified for that interface when this route comes back into service. This feature is useful when it is preferable to close down a backup route quickly when a primary route comes back into service.

Wait for s seconds after power up before allowing this route to activate the interface
The value in this text box specifies the delay that the router should wait after power-up before packets matching this route will initiate a connection of the interface configured in the route. It is typically used on W-WAN routers that have ISDN backup in order to prevent unnecessary ISDN connections from being made whilst a W-WAN connection is first being established.

Mark this route as "Out of Service" in the interface fails to connect after n consecutive attempts
Normally, if an interface is requested to connect by a route and fails to connect, the route metric is set to 16 for the period of time specified by the **Mark a static route as "Out Of Service" for s seconds** parameter on the ***Configuration – Network > IP Routing/Forwarding > IP Routing*** page. If the value in this text box is non-zero, the route metric will not be set to 16 until the number of connection attempts specified by this parameter have been made.

If the interface fails to connect, try again in s seconds
If an interface is requested to connect by this route (due to IP traffic being present) and it fails to connect, the route will be marked as out of service but the router will continue to attempt to connect at the interval specified by the value in this text box. If the interface does connect, the router will clear the out of service status for the route.

Deactivate the interface after it successfully connects
When checked, this check box will cause the router to deactivate an interface once a successful activation attempt has been made. This is used in conjunction with the above retry parameter. If the above retry parameter is not set, this checkbox is "greyed out".

Do not allow this interface to be activated by this route for s seconds after the last activation attempt
The value in this text box is the delay to wait before re-initiating a connection after it has dropped whilst still required.

Only queue one packet whilst waiting for the interface to connect
When checked, this checkbox will cause the router to enqueue only one packet while waiting for the interface to connect. When unchecked, the router will enqueue two packets.

When this route becomes available, deactivate the following interfaces x,y x,y
The interfaces specified by the values in these two pairs of drop-down list and text boxes will be deactivated when this route becomes available again after being out of service. This feature is typically used to deactivate backup interfaces when the primary interface becomes available after being out of service. Select the required interface from the drop-down list and enter the interface instance number into the text box as usual.

When this route becomes unavailable, remove the "Out of Service" state on x,y
This drop-down list and text box are used to specify the interface (available options are "None", "PPP", "Ethernet" and "Tunnel") and instance that should be taken out of the "Out of Service" state when the interface that this route is configured to use is deactivated.

Keep this route in service for s seconds after OOS state is cleared
When this checkbox is checked, the following text box is enabled (i.e. it is no longer "greyed out"), allowing a value to be entered. The value specifies the period that the interface specified above will remain in service even though it is actually unable to pass traffic immediately. This is behaviour useful in situations where a PPP interface is activating and traffic should not try the next interface until this one has been allowed a certain amount of time to come up. When this timer expires, if the interface is unable to pass traffic, it will be marked Out of Service and the next interface will be tried.

Assign this route to recovery group n
The value in this text box is used to assign the route to a "recovery group". This means that if all the routes in a particular recovery group go out of service, the out of service status is cleared for all routes in that group. If one route in a group comes back into service, all routes with a lower priority (metric) also have their out of service status cleared.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
route	n	metric	0 – 2147483647	Use metric n when the interface is not active
route	n	srcip	Valid IP address a.b.c.d	IP Address a.b.c.d
route	n	srcmask	Valid netmask a.b.c.d	Mask a.b.c.d
route	n	inrip	on,off	Include this route in RIP advertisements
route	n	doinact2	on,off	Make PPP n interface use the alternative idle timeout when this route becomes available
route	n	inact2add	0 – 2147483647	Make PPP n interface use the alternative idle timeout when this route becomes available
route	n	pwr_dly	0 - 255	Wait for s seconds after power up before allowing this route to activate the interface
route	n	actooslim	0 – 2147483647	Mark this route as "Out Of Service" if the interface fails to connect after n consecutive attempts
route	n	chkoos_int	0 – 2147483647	If the interface fails to connect, try again in s seconds
route	n	chkoos_deact	0 - 255	Deactivate the interface after it successfully connects
route	n	dial_int	0 – 255 Default 10	Do not allow this interface to be activated by this route for s seconds after the last activation attempt
route	n	q1	on,off	Only queue one packet whilst

Entity	Instance	Parameter	Values	Equivalent Web Parameter
				waiting for the interface to connect
route	n	deact_ent	Blank,PPP	When this route becomes available, deactivate the following interfaces x,y
route	n	deact_add	0 – 2147483647	When this route becomes available, deactivate the following interfaces x,y
route	n	deact_ent2	Blank,PPP	When this route becomes available, deactivate the following interfaces x,y
route	n	deact_add2	0 – 2147483647	When this route becomes available, deactivate the following interfaces x,y
route	n	unoos_secs	0 – 2147483647	Keep this route in service for s seconds after OOS state is cleared
route	n	rgroup	0 - 255	Assign this route to recovery group n

Default Route n

Configuration – Network > IP Routing/Forwarding> Static Routes> Default Route n

The following two web pages and associated command line commands are used to set up default IP routes that will be used to route non-local IP addresses not specified in a static route. The parameters are identical to those on the static route pages with the exception that there are no IP address or Mask parameters.

Description
The text in this text box is used to assign a convenient and memorable description for the route.

Default route via:

Gateway a.b.c.d
As per equivalent parameter in Routes n.

Interface x,y
As per equivalent parameter in Routes n.

Metric n
As per equivalent parameter in Routes n.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
def_route	n	descr	Up to 20 characters	Description
def_route	n	gateway	Valid IP address a.b.c.d	Gateway a.b.c.d

Entity	Instance	Parameter	Values	Equivalent Web Parameter
def_route	n	ll_ent	Blank,PPP,ETH,TUN	Interface x,y
def_route	n	ll_add	0 – 2147483647	Interface x,y
def_route	n	upmetric	1 - 16	Metric

Advanced

Configuration – Network > IP Routing/Forwarding> Static Routes> Default Route n> Advanced

Use metric n when the interface is not active
As per equivalent parameter in Routes n.

Use this route only if the source IP address of the packet matches
As per equivalent parameter in Routes n.

IP address a.b.c.d
As per equivalent parameter in Routes n.

Mask a.b.c.d
As per equivalent parameter in Routes n.

Include this route in RIP advertisements
As per equivalent parameter in Routes n.

Make PPP x interface use the alternative idle timeout when this route becomes available
As per equivalent parameters in Routes n.

Wait for s seconds after power up before allowing this route to activate the interface
As per equivalent parameter in Routes n.

If the interface is configured for "dial on demand"

Mark this route as "Out Of Service" if the interface fails to connect after n consecutive attempts
As per equivalent parameter in Routes n.

If the interface fails to connect, try again in s seconds
As per equivalent parameter in Routes n.

Deactivate the interface after it successfully connects
As per equivalent parameter in Routes n.

Do not allow this interface to be activated by this route for s seconds after the last activation attempt
As per equivalent parameter in Routes n.

Only queue one packet whilst waiting for the interface to connect
As per equivalent parameter in Routes n.

When this route becomes available, deactivate the following interfaces x,y x,y
As per equivalent parameter in Routes n.

When this route becomes unavailable, remove the "Out Of Service" state on x,y
As per equivalent parameter in Routes n.

Keep this route in service for s seconds after OOS state is cleared

As per equivalent parameter in Routes n.

Assign this route to recovery group n
As per equivalent parameter in Routes n.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
def_route	n	metric	0 – 2147483647	Use metric n when the interface is not active
def_route	n	srcip	Valid IP address a.b.c.d	IP Address a.b.c.d
def_route	n	srcmask	Valid netmask a.b.c.d	Mask a.b.c.d
def_route	n	inrip	on,off	Include this route in RIP advertisements
def_route	n	doinact2	on,off	Make PPP n interface use the alternative idle timeout when this route becomes available
def_route	n	inact2add	0 – 2147483647	Make PPP n interface use the alternative idle timeout when this route becomes available
def_route	n	pwr_dly	0 - 255	Wait for s seconds after power up before allowing this route to activate the interface
def_route	n	actooslim	0 – 2147483647	Mark this route as “Out Of Service” if the interface fails to connect after n consecutive attempts
def_route	n	chkoos_int	0 – 2147483647	If the interface fails to connect, try again in s seconds
def_route	n	chkoos_deact	0 – 2147483647	Deactivate the interface after it successfully connects
def_route	n	dial_int	0 – 255 Default 10	Do not allow this interface to be activated by this route for s seconds after the last activation attempt
def_route	n	q1	on,off	Only queue one packet whilst waiting for the interface to connect
def_route	n	deact_ent	Blank,PPP	When this route becomes available, deactivate the following interfaces x,y
def_route	n	deact_add	0 – 2147483647	When this route becomes available, deactivate the following interfaces x,y

Entity	Instance	Parameter	Values	Equivalent Web Parameter
def_route	n	deact_ent2	Blank,PPP	When this route becomes available, deactivate the following interfaces x,y
def_route	n	deact_add2	0 – 2147483647	When this route becomes available, deactivate the following interfaces x,y
def_route	n	unoos_secs	0 – 2147483647	Keep this route in service for s seconds after OOS state is cleared
def_route	n	rgroup	0 - 255	Assign this route to recovery group n

RIP

Configuration – Network > IP Routing/Forwarding> RIP

The web pages and command line commands described in this section control the configuration of the routing Information Protocol (RIP) functionality of the router.

Global RIP Settings

Configuration – Network > IP Routing/Forwarding> RIP> Global RIP Settings

Enable RIP
When checked, this checkbox enables the RIP functionality.

Send RIP advertisements every s seconds
The value in this text box specifies the interval between sending RIP packets. These packets contain the current routes held by the router (e.g. any active PPP routes), static routes and the default route. A value of 0 disables sending.

Mark routes as unusable if we don't get advertisements for s seconds
The value in this text box specifies the time for which an updated metric will apply when a RIP update is received. If no updates are received within this period, the usual metric will take over.

Delete routes after another s seconds
The value in this text box specifies the length of time that the router will continue to advertise this route when a RIP update timeout occurs and the route metric is 16. This behaviour is designed to help propagate the dead route to other routers. The router will no longer use a metric advertised by a RIP update if the route has been set out of service locally.

Allow RIP to update static routes
When checked, this checkbox allows an incoming, matching RIP update to change the metric of the static route. This happens when the update matches a configured static route.

Enable Poison Reverse
When checked, this checkbox enables poison reverse, to notify when a neighbouring router is unavailable.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
rip	n	enable	on,off	Enable RIP
rip	n	interval	0 - 2147483647	Send RIP advertisement every s seconds
rip	n	ripto	0 - 2147483647	Mark routes as unusable if we don't get advertisement for s seconds
rip	n	riplingerto	0 - 2147483647	Delete routes after another s seconds
rip	n	updatestatic	on,off	Allow RIP to update static routes
rip	n	poisonreverse	on,off	Enable Poison Reverse

Access Lists

Configuration – Network > IP Routing/Forwarding> RIP> Global RIP Settings> Access Lists

The router has the ability to modify route metrics based upon received RIP responses. Static routes and default routes will have their metric modified if the route fits within one of the routes found within the RIP packet. For Ethernet routes, the gateway for the route will be set to the source address of the RIP packet. The route modifications will be enforced for 180 seconds unless another RIP response is received within that time.

RIP packets must have a source address that is included in the RIP access list.

Adding permitted IP addresses to the access list is controlled using a table with the single parameter described below.

IP Address a.b.c.d
The value in this text box is the IP address to be added to the list of IP addresses that RIP packets must come from if they are to modify route metrics. Up to ten IP addresses may be added. The **Add** and **Delete** buttons work in the usual way for configuration tables.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
riprx	0 - 9	IPaddr	Valid IP address a.b.c.d	IP Address a.b.c.d

Authentication Keys

Configuration – Network > IP Routing/Forwarding> RIP> Global RIP Settings> Authentication Keys

RIP authentication keys are used with the "plain password" and MD5 RIP authentication methods.

Authentication Key n

Key k
The value in this text box is the RIP authentication key. Enter a string of up to 16 characters long. A current key will not be displayed.

Confirm Key

Re-enter the new key into this text box to allow the router to check that the two are identical.

Key ID (MD5 only)
The value in this text box is the ID for the key. The ID is inserted into the RIP packet when using RIP v2 MD5 authentication and is used to look up the correct key for received packets. The valid range is 0 – 255.

Valid from now / dd,mm,yy
These two radio buttons select, between having the validity period for the key starting immediately of allowing a start date to be defined. The starting date is specified using a drop down list to select the start day, a drop-down list to select the start month and a text box to enter the start year. Selecting the "Disable" option from the day and "None" from the month means that this key should not be used. The year can be specified as either two or four digits (e.g. 11 or 2011).

Expires Never / dd,mm,yy
These two radio buttons select between defining the end date using the drop-down lists and text box or by setting the expiration to "Never". The key end day is selected from the first drop down list, selecting "Disable" means that the key should not be used. The end month is selected from the second drop-down list, selecting "None" means that the key should not be used. The year is entered into the text box and can be in two or four digit format.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ripauth	0 - 9	key	Up to 16 characters	Key k
ripauth	0 – 9	keyid	0 - 255	Key ID
ripauth	0 – 9	sday	0 - 31	Valid from d,m,y
ripauth	0 – 9	smon	0 - 12	Valid from d,m,y
ripauth	0 – 9	syear	0 – 65535	Valid from d,m,y
ripauth	0 – 9	eday	0 - 31	Expires d,m,y
ripauth	0 – 9	emon	0 - 12	Expires d,m,y
ripauth	0 - 9	eyear	0 – 65535	Expires d,m,y

Interfaces

Configuration – Network > IP Routing / Forwarding > RIP> Interfaces

This section describes the parameter of ***Configuration – Network > IP Routing / Forwarding > RIP> Interfaces*** submenu.

Ethernet / PPP / GRE

Configuration – Network > IP Routing / Forwarding > RIP> Interfaces> Ethernet/PPP/GRE

The configuration in these three sub-menus is identical.

Send RIP advertisements on this interface
Check this box to enable rip and to reveal further configuration parameters below.

Use RIP:
Select from the values 'v1', 'v2' and 'v1 Compatible' in the dropdown list. When RIP version is set to 'V1' or 'V2', the unit will transmit RIP version 1 or 2 packets respectively (version 2 packets are sent to the "all routers" multicast address 224.0.0.9). When RIP Version is set to "V1 Compat", the unit will transmit RIP version 2 packets to the subnet broadcast address. This allows 'V1' capable routers to act upon these packets.

Send RIP advertisements as:

Broadcasts:
RIP packets are by default sent out on a broadcast basis or to a multi-cast address. Do not change this parameter unless you intend to alter this behaviour.

Multicasts (Only visible when 'v2' is selected in the 'Use RIP' option above):
This is automatically selected for sending to the default RIP v2 multicast address 224.0.0.9.

<BLANK BOX>
This parameter may be used to force RIP packets to be sent to a specified IP or multicast address. It is particularly useful if you need to route the packets via a VPN tunnel. By default Broadcasts/multicasts are selected – depending on your RIP version.

Use Authentication:
This parameter selects the authentication method for RIP packets. Selection is by clickable radio button. Only one option is enabled multiple selections are not possible.

None:
When set to "Off", the interface will send and receive packets without any authentication.

Access list:
When set to "Access List", the interface will send RIP packets without any authentication. When receiving packets, the interface will check the sender's IP address against the list entered on the ***Configuration – Network > IP Routing / Forwarding > RIP > Global RIP settings > Access Lists*** page, and if the IP address is present in the list, the packet will be allowed through.

Plain password:
When set to "Plain password (V1+V2)", the interface will use the first valid key it finds (set on the ***Configuration – Network > IP Routing / Forwarding > RIP > Global RIP settings > Authentication Keys > Authentication Key n*** pages), and use the plaintext RIP authentication method before sending the packet out. If no valid key can be found, the interface will not send any RIP packets. When receiving a RIP packet, a valid plaintext key must be present in the packet before it will be accepted. This method can be used with both RIP v1 and RIP v2.

MD5:
When set to "MD5 (V2 only)", the interface will use the first valid key it finds (set on the ***Configuration – Network > IP Routing / Forwarding > RIP > Global RIP settings > Authentication Keys > Authentication Key n*** pages), and use the MD5 authentication algorithm before sending the packet out. If no valid key can be found, the interface will not send any RIP packets. Received RIP packets must be authenticated using the MD5 authentication algorithm before they will be accepted. This method can be used with RIP v2.

Only send RIP advertisements when this interface is in service:

Select this parameter for RIP advertisements only to be sent when the interface is in the UP state in the routing table.

Use Triggered RIP on this interface:

Enable triggered RIP (RFC2091). When triggered RIP is enabled, RIP timers are disabled.

Include this interface in Rip advertisements:

Select to cause the subnet configured on this interface to not be advertised by RIP.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
tun	n	rip	0,1	Enable RIP = 1 Disable RIP = 0
tun	n	ripip	Valid IP address a.b.c.d	Unicast RIP update address
tun	n	ripauth	0-3	0 = None 1 = Access List 2 = Plain Password 3 = MD5 v2 only
tun	n	ripis	on,off	Turn on to send updates only when in service
tun	n	inrip	on,off	Include interface subnet in RIP advertisements
tun	n	triggeredrip	on,off	Enable RIP RFC2091

OSPF

Configuration – Network > IP Routing / Forwarding > OSPF

Open Shortest Path First (OSPF) is an Interior Gateway Protocol (IGP) developed for IP networks based on the shortest path first or link-state algorithm.

The router uses link-state algorithms to send routing information to all nodes in a network by calculating the shortest path to each node based on a topography of the network constructed by each node. Each router sends that portion of the routing table that describes the state of its own links and the complete routing structure (network topography).

The advantage of the shortest path first algorithms is that they result in smaller, more frequent update everywhere. They converge quickly, thus preventing such problems as routing loops and Count-to-Infinity (where routers continuously increment the hop count to a particular network). This makes for a stable network.

In order to use OSPF on the router, a valid configuration file must exist in the router's filing system.

Enable OSPF
When checked, this checkbox reveals the following parameters:

OSPF Configuration Filename
The file that contains the configuration data for OSPF is selected from this drop-down list. The file should have a ".conf" extension.

Load Config file

When this button is clicked, the router attempts to load the file specified in the file selection list box into the edit window below the button. The text in the window can be edited as required.

Save Config File
When this button is clicked, the text in the edit window will be saved to the filename specified in the drop-down list above. These three controls allow an OSPF configuration file to be loaded, edited and saved.

Restart OSPF after configuration file is saved
When checked, this checkbox will cause the OSPF functions to restart once the edited configuration file has been saved.

Restart OSPF if a fatal error occurs
When checked this checkbox will cause OSPF functioning to restart after a delay of 5 seconds if a fatal error occurs.

OSPF Tracing
In common with some of the other functionality of the router, OSPF supports some debug functionality. The amount of information in the debug traces is controlled from this drop-down list. The available levels are “Off”, “Low”, “Med” and “High”. Selecting “Off” disables debug tracing.

Ignore MTU indications
All OSPF routers must have the same Maximum Transmitted Unit (MTU) and this value is advertised in the OSPF packets. When checked, this checkbox will cause the router to ignore received packets that have a MTU that differs from that of the router itself.

Use Interface IPsec source IP
When checked, this checkbox will cause OSPF functions to use the source IP address of the interface specified in ***Configuration – Network > Interfaces > Advanced > PPP n*** **: Use interface x,y for the source IP address of IPsec packets** on the interface being used. When unchecked, OSPF will use the source IP address of the interface being used for its source address.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ospf	0	Enable	on,off	Enable OSPF
ospf	0	conffile		OSPF Configuration Filename
ospf	0	new_cfg_rest	on,off	Restart OSPF after a configuration file is saved
ospf	0	fatal_rest	on,off	Restart OSPF if a fatal error occurs
ospf	0	debug	0 – 3 0 = Off 1 = Low 2 = Med 3 = High	OSPF Tracing
ospf	0	ignore_mtu	on,off	Ignore MTU indications
ospf	0	useipsecent	on,off	Use Interface IPsec source IP

BGP

Configuration – Network > IP Routing / Forwarding > BGP

The Border Gateway Protocol (BGP) routing protocol is supported by TransPort routers. This page contains the configuration parameters used to control the behaviour of BGP. Most of the configuration is controlled by a configuration file (raw text) named bgp.cnf. This file would normally be created in a text editor on a computer and loaded onto the router. The router contains a simple editor that can be used to modify the file. The configuration parameters described here mainly define what action is to be taken when errors occur and specify the configuration file to be used.

Enable BGP
When checked, this checkbox enables BGP routing.

BGP Configuration Filename
The configuration file to use is selected from this drop-down list. The default filename is bgp.cnf. An error message will be displayed if the specified file cannot be found.

Load Config file
Click this button to load the file specified from the drop-down list. The contents of the file will be visible in the edit window which appears below the button.

Save Config File

If the edit functions are used to modify the file, it can be saved back to the filing system by clicking this button.

Restart BGP after configuration file is saved
When checked, this checkbox will cause the router to restart routing using BGP after the file has been saved using the above **Save** button.

Restart BGP if a fatal error occurs
When checked, this checkbox will cause the router to restart routing using BGP if a fatal error occurs.

Advertise non-connected networks
When checked, this checkbox will cause BGP to advertise networks that exist in the BGP configuration file but that are not actually a connected network or interface.

BGP Tracing
As with OSPF, the level of debug tracing information is selected from this drop-down list. The available levels are; “Off”, “Low”, “Med” and High.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
bgp	0	enable	on,off	Enable BGP
bgp	0	conffile		BGP Configuration Filename
bgp	0	new_cfg_rest	on,off	Restart BGP after configuration file is saved
bgp	0	fatal_rest	on,off	Restart BGP if a fatal error occurs
bgp	0	allow_non_nets	on,off Default ON	Advertise non-connected networks
bgp	0	debug	0 - 3	BGP Tracing

IP Port Forwarding / Static NAT Mappings

Configuration – Network > IP Routing / Forwarding > IP Routing /Static NAT Mappings

The router supports Network Address Translation (NAT) and Network Address and Port Translation (NAPT). NAT or NAPT may be enabled on a particular interface such as a PPP instance. When operating with NAT enabled, this interface has a single externally visible IP address. When sending IP packets, the local IP addresses (for example on a local area network) are replaced by the single IP address of the interface. The router keeps track of the local IP addresses and port numbers so that if a matching reply packet is received, it is directed to the correct local IP address. With only one externally visible IP address, NAT effectively prevents external computers from addressing specific local hosts, thus providing a very basic level of "firewall" security.

Static NAT mappings allow received packets destined for particular ports to be directed to specific local IP addresses. For example, to have a server, running on a local network, externally accessible, a static NAT mapping would be set up using the local IP address of the server and the port number used to access the required service.

Configuring IP port forwarding and static NAT mapping is done by entering the following configuration values into a table and using the Add button to add them into the NAT configuration for the router.

External Min Port
The value in this text box specifies the lowest port number to be redirected.

External Max Port
The value in this text box specifies the highest port number to be redirected.

Forward to Internal IP Address a.b.c.d
The value in this text box is the IP address to which packets containing the specified destination port number are to be redirected.

Forward to Internal Port
The value in this text box specifies the IP port number to which packets containing the specified port number are to be redirected. When set to "0", no port remapping occurs and the original port number is used. The NAT mode parameter of the appropriate interface must be set to "NAPT" rather than "NAT" or "OFF" for this parameter to take effect.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
nat	0 - 29	minport	0 - 65535	External Min Port
nat	0 - 29	maxport	0 - 65535	External Max Port
nat	0 - 29	IPaddr	Valid IP address a.b.c.d	Forward to Internal IP Address a.b.c.d
nat	0 - 29	mapport	0 - 65535	Forward to Internal Port

Command format:

Nat <entry> <parameter> <value>

Example commands:

To set the IP address for entry 0 in the table to 10.1.2.10 enter the command:

nat 0 IPaddr 10.1.2.10

Multicast Routes

Configuration – Network > IP Routing / Forwarding > Multicast Routes

Digi TransPort routers support multicast routes, allowing them to route packets to multicast group addresses. Up to 20 different static multicast routes may be configured.

Static multicast routes must be used in conjunction with the IGMP parameter on the outbound interface. For example, after configuring a static multicast route for multicast traffic via PPP 1, the **IGMP** parameter in ***Configuration – Network > Interfaces > IGMP*** needs setting to ON. Multicast routing is configured using a table with the following parameters:

Multicast Address a.b.c.d
The value in this text box is used in conjunction with the Mask parameter below, to specify the destination multicast group address for packets that will match this route. So, if a router receives a packet with a destination multicast group address that matches the specified Multicast Address/Mask combination, it will route that packet through the interface specified by the Interface parameters below.

Mask a.b.c.d
The value in this text box is the address mask that is used in conjunction with the Multicast Address parameter as described above.

Interface x,y
These two parameters in the drop-down list and adjacent text box specify the interface and interface instance used to route packets matching the Multicast Address/Mask combination. The options available in the drop-down list are; PPP, Ethernet, Tunnel.

Enable multicast source path checking
When checked, this checkbox

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
mcast	0 - 19	IPaddr	Valid IP address a.b.c.d	Multicast Address a.b.c.d
mcast	0 - 19	mask	Valid IP address a.b.c.d	Mask a.b.c.d
mcast	0 - 19	ll_ent	PPP,ETH,TUN	Interface x,y
mcast	0 - 19	ll_add	Valid interface number 0 - 2147483647	Interface x,y

Virtual Private Networking (VPN)

Configuration – Network > Virtual Private Network (VPN)

The ***Configuration – Network > VPN*** menu has the following sub-menu options:

- IPsec
- L2TP
- PPTP
- OpenVPN

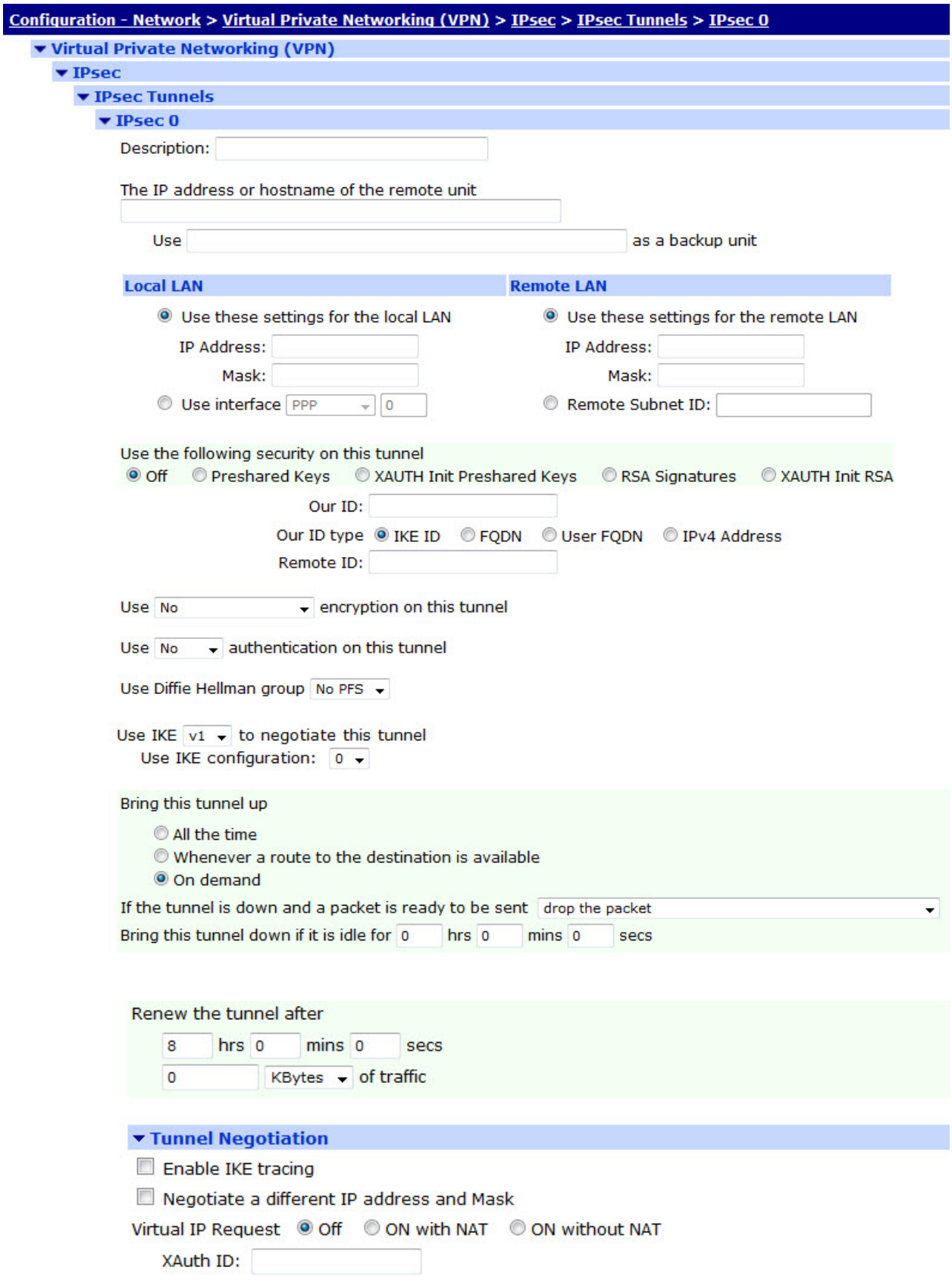
IPsec

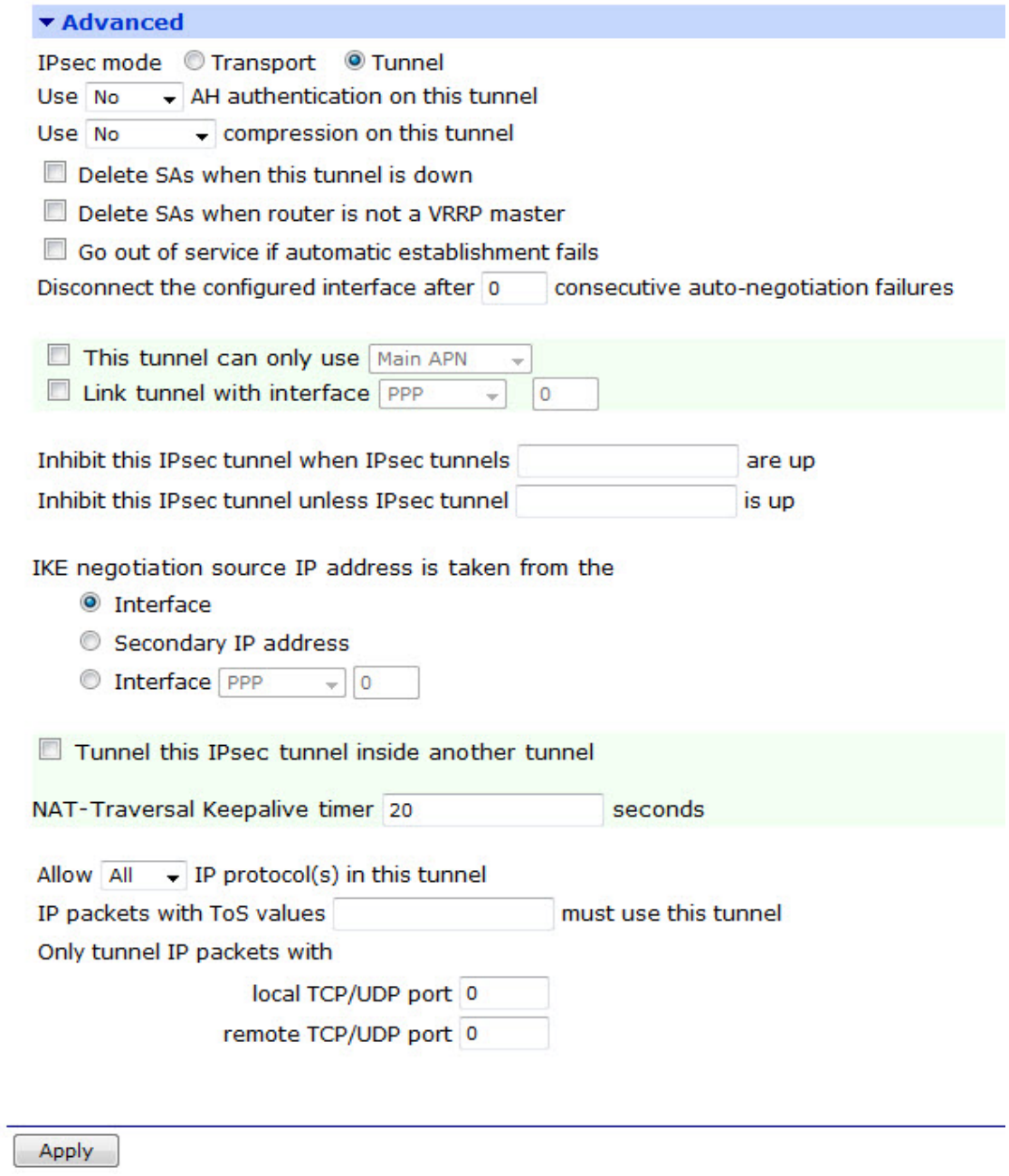
Configuration – Network > Virtual Private Network (VPN)> IPsec

IPsec (Internet Protocol security) refers to a group of protocols and standards that may be used to protect data during transmission over the internet (which is inherently insecure). Various levels of support for IPsec can be provided on the router depending on the model. The web pages located under the ***Configuration – Network > Virtual Private Networking (VPN) > IPsec*** are used to set the various parameters and options that are available. You should note however that this is a complex area and you should have a good understanding of user authentication and data encryption techniques before you commence. For further information refer to the "IPsec and VPNs" section in this manual. Also check the Technical Notes section of the Digi International web site at www.digi.com for the latest IPsec application notes.

The ***Configuration – Network > Virtual Private Networking (VPN) > IPsec*** menu has the following sub-menu options:

- IPsec Tunnels
- Tunnel Negotiation
- Advanced
- IPsec Default Action
- IPsec Groups
- Dead Peer Detection
- IKE
- IKEv2


Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec 0
Virtual Private Networking (VPN)
IPsec
IPsec Tunnels
IPsec 0
Description:
The IP address or hostname of the remote unit
Use as a backup unit
Local LAN
Remote LAN
Use these settings for the local LAN
IP Address:
Mask:
Use interface PPP 0
Use these settings for the remote LAN
IP Address:
Mask:
Remote Subnet ID:
Use the following security on this tunnel
Off
Preshared Keys
XAUTH Init Preshared Keys
RSA Signatures
XAUTH Init RSA
Our ID:
Our ID type
IKE ID
FQDN
User FQDN
IPv4 Address
Remote ID:
Use No encryption on this tunnel
Use No authentication on this tunnel
Use Diffie Hellman group No PFS
Use IKE v1 to negotiate this tunnel
Use IKE configuration: 0
Bring this tunnel up
All the time
Whenever a route to the destination is available
On demand
If the tunnel is down and a packet is ready to be sent drop the packet
Bring this tunnel down if it is idle for 0 hrs 0 mins 0 secs
Renew the tunnel after
8 hrs 0 mins 0 secs
0 KBytes of traffic
Tunnel Negotiation
Enable IKE tracing
Negotiate a different IP address and Mask
Virtual IP Request
Off
ON with NAT
ON without NAT
XAuth ID:


Advanced
IPsec mode Transport Tunnel
Use No AH authentication on this tunnel
Use No compression on this tunnel
Delete SAs when this tunnel is down
Delete SAs when router is not a VRRP master
Go out of service if automatic establishment fails
Disconnect the configured interface after 0 consecutive auto-negotiation failures
This tunnel can only use Main APN
Link tunnel with interface PPP 0
Inhibit this IPsec tunnel when IPsec tunnels are up
Inhibit this IPsec tunnel unless IPsec tunnel is up
IKE negotiation source IP address is taken from the
Interface
Secondary IP address
Interface PPP 0
Tunnel this IPsec tunnel inside another tunnel
NAT-Traversal Keepalive timer 20 seconds
Allow All IP protocol(s) in this tunnel
IP packets with ToS values must use this tunnel
Only tunnel IP packets with
local TCP/UDP port 0
remote TCP/UDP port 0
Apply

The first stage in establishing a secure link between two endpoints on an IP network is for those two points to securely exchange a little information about each other. This enables the endpoint responding to the request to decide whether it wishes to enter a secure dialogue with the endpoint requesting it. To achieve this, the two endpoints commonly identify themselves and verify the identity of the other party. They must do this in a secure manner so that the process cannot be “listened in to” by any third party. The IKE protocol is used to perform this “checking” and if everything matches up it creates a Security Association (SA) between the two endpoints, normally one for data being sent TO the remote end and one for data being received FROM it.

Once this initial association exists the two devices can “talk” securely about and exchange information on what kind of security protocols they would like to use to establish a secure data link, i.e. what sort of encryption and/or authentication they can use and what sources/destinations they will accept. When this second stage is complete (and provided that both systems have agreed what they will do), IPSec will have set up its own Security Associations which it uses to test incoming and outgoing data packets for eligibility and perform security operations on before passing them down or relaying them from the “tunnel”.

IPsec Tunnels > IPsec n

Configuration – Network > Virtual Private Network (VPN)>IPsec> IPsec Tunnels> IPsec n

Once the IKE parameters have been set-up, the next stage is to define the characteristics of the IPsec tunnels, or encrypted routes. This includes items such as what source and destination addresses will be connected by the tunnel and what type of encryption and authentication procedures will be applied to the packets being tunnelled. For obvious reasons it is essential that parameters such as encryption and authentication are the same at each end of the tunnel. If they are not, then the two systems will not be able to agree on what set of rules or “policy” to adopt for the IPsec tunnel and communication cannot take place.

Description
This parameter allows you to enter a name for IPsec tunnel to make it easier to identify.

The IP address or hostname of the remote unit
The IP address or hostname of the remote IPsec peer that a VPN will be initiated to.

Use a.b.c.d as a backup unit
The IP address or hostname of a backup peer. If the router cannot open a connection to the primary peer, this configuration will be used. Please note that the backup peer device must have an identical IPsec tunnel configuration as the primary peer.

Use these settings for the local LAN
These define the local LAN subnet settings used on the IPsec tunnel.

IP Address
Use this IP address for the local LAN subnet. This is usually the IP address of the router’s Ethernet interface or that of a specific device on the local subnet (such as a PC running a client or host application).

Mask
Use this IP mask for the local LAN subnet. The mask sets the range of IP addresses that will be allowed to use the IPsec tunnel.

Use interface x,y
Use the IP address and mask of the specified interface.

Use these settings for the remote LAN
These define the remote LAN subnet settings used on the IPsec tunnel.

IP Address
Use this IP address for the remote LAN subnet. This is usually the IP address of the peer’s Ethernet interface or that of a specific device on the local subnet (such as a PC running a client or host application).

Mask

Use this IP mask for the remote LAN subnet. The mask sets the range of IP addresses that will be allowed to use the IPsec tunnel.

Remote Subnet ID
Normally used with L2TP/IPsec VPNs. When the router is in server mode and negotiating IPsec from behind a NAT box, this parameter should be configured to the ID sent by the remote Windows client (this is usually the computer name).

Use the following security on this tunnel
These define the security identities used on the IPsec tunnel.

Preshared Keys	Requires that both IPsec peers share a secret key, or password, that can be matched by and verified by both peers. To configure the PSK, a user will need configuring that matches the inbound ID of the remote peer and the PSK is configured using the password parameter. This is done via ***Configuration – Security > Users***. The User configuration serves a dual purpose in that it may contain entries for normal login access (e.g. HTTP, FTP or Telnet) and entries for IPsec tunnels.
XAUTH Init Preshared Keys	Used when the remote peer is a Cisco device using XAUTH and PSK authentication.
RSA Signatures	Select this option when the IPsec authentication will use X.509 certificates.
XAUTH Init RSA	Used when the remote peer is a Cisco device using XAUTH and X.509 certificates for authentication.

Our ID
When Aggressive mode is On, this parameter is a string of up to 20 characters. It is sent to the remote peer to identify the initiator (e.g. the router). The variable **%s** can be used in this parameter which will cause the router's serial number to be sent. It can be prefixed with other text if required.
When certificates are being used, this parameter should be configured with the "Altname" field in a valid certificate held on the router.

Our ID type
This defines how the remote peer is to process the ***Our ID*** configuration.

IKE ID	The Our ID parameter is a simple key ID (e.g. vpnclient1).
FQDN	The Our ID parameter is a Fully Qualified Domain Name (e.g. vpnclient1.anycompany.com)
User FQDN	The Our ID parameter is a Fully Qualified Domain Name with a user element (e.g. joe.bloggs@anycompany.com)
IPv4 Address	An IPv4 Address in dotted decimal notation.

Remote ID
When Aggressive mode is On, this parameter is a string of up to 20 characters which is used to identify the remote peer. It should contain the same text as the ***Our ID*** parameter in the **remote peer**'s configuration.
When Aggressive mode is Off, this parameter must be the IP address of the remote peer.

RSA Key File

This parameter can be used to override the private key filename in the IKE configuration. It is only used when RSA Signatures (Certificates) are being used for the authentication stage of the IKE negotiation.

Use enc encryption on this tunnel
The ESP encryption protocol to use with this IPsec tunnel. The options are:

- No (None)
- Null
- DES
- 3DES
- AES (128 bit keys)
- AES (192 bit keys)
- AES (256 bit keys)

If the dropdown options only display None and Null, the router will need Encryption enabling. Please speak to your sales contact with regards to getting Encryption enabled.

Use auth authentication on this tunnel
The ESP authentication algorithm to use with this IPsec tunnel. The options are:

- No (None)
- MD5
- SHA1

Use Diffie Hellman group
The Diffie Hellman (DH) group to use when negotiating new IPsec SAs. When used, the IPsec SA keys cannot be predicted from any of the previous keys generated. The options are “No PFS”, 1, 2 or 3. The larger values result in “stronger” keys but they take longer to generate.

Use IKE n to negotiate this tunnel
The IKE version to use to negotiate this IPsec tunnel.

Use IKE configuration
The IKE configuration instance to use with this Eroute when the router is configured as an Initiator.

Bring this tunnel up
This controls how the IPsec tunnel is brought up. The options are:

- All the time
- Whenever a route to the destination is available
- On demand

If the tunnel is down and a packet is ready to be sent
Defines the action that is performed when the IPsec tunnel is down and a packet needs to be sent. The options are:

- Bring the tunnel up
- Drop the packet
- Send the packet without encryption and authentication

Bring this tunnel down if it is idle for h hrs m mins s secs
This parameter is used when the IPsec tunnel is configured to come up on demand and defines how long the IPsec tunnel should remain up if there is no traffic is being sent on the tunnel.

Renew the tunnel after
Defines the constraints of when the IPsec tunnel SA has to be renewed.

h hrs m mins s secs
Re-new the IPsec SA after the specified amount of time.

n units of traffic
Re-new the IPsec SA after the specified amount of traffic has been passed over the tunnel.
The units can be Kbytes, Mbytes or Gbytes.
A value of 0 means that this parameter will not be used and SAs will expire and be renewed based time, rather than amount of traffic.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eroute	n	descr	String	Description
eroute	n	peerip	IP address or hostname	The IP address or hostname of the remote unit
eroute	n	bakpeerip	IP address or hostname	Use n as a backup unit
eroute	n	locip	IP address	IP Address (for Local LAN)
eroute	n	locmsk	IP Mask	IP Mask (for Local LAN)
eroute	n	locipifent	blank, ETH, PPP	Use interface x,y x = Interface type
eroute	n	locipifadd	Integer	Use interface x,y y = interface number
eroute	n	remip	IP address	IP Address (for Remote LAN)
eroute	n	remmsk	IP Mask	IP Mask (for Remote LAN)
eroute	n	remnetid	String	Remote Subnet ID
eroute	n	authmeth	Off, Preshared, xauthinitpre, rsa, xauthinitrsa	Use the following security on this tunnel
eroute	n	ourid	String	Our ID
eroute	n	ouridtype	0 = IKE ID 1 = FQDN 2 = User FQDN 3 = IPv4 Address	Our ID type
eroute	n	peerid	String	Remote ID
eroute	n	privkey	Filename	RSA Key File

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eroute	n	espenc	off, null, des, 3des, aes	Use enc encryption on this tunnel
eroute	n	enckeybits	128, 192, 256	Use enc encryption on this tunnel
eroute	n	espauth	off, md5, sha1	Use auth authentication on this tunnel
eroute	n	dhgroup	0, 1, 2, 3	Use Diffie Hellman group
eroute	n	ikever	1, 2	Use IKE n to negotiate this tunnel
eroute	n	ikecfg	0, 1	Use IKE configuration
eroute	n	autosa	0 = On Demand 1 = When a route to the destination is available 2 = All the time	Bring this tunnel up
eroute	n	nosa	drop, pass, try	If the tunnel is down and a packet is ready to be sent
eroute	n	inact_to	Integer	Bring this tunnel down if it is idle for h hrs m mins s secs This CLI value is entered in seconds only.
eroute	n	ltime	Integer	Renew the tunnel after h hrs m mins s secs This CLI value is entered in seconds only.
eroute	n	lkbytes	Integer	Renew the tunnel after n units of traffic. This CLI value is entered in Kbytes only.

Tunnel Negotiation

Configuration – Network > Virtual Private Network (VPN)>IPsec> IPsec Tunnels> IPsec n> Tunnel Negotiation

Enable IKE tracing
This will enable the router to write IKE negotiation information in the analyser trace.

Negotiate a different IP address and Mask
The IPsec tunnel can be configured to negotiate a different local LAN IP address and mask. The firewall can then be used to translate the source addresses of the packets to a value that lies within the negotiated range. This is so that a packet can match more than one IPsec tunnel but will use a different source address (from the peer's perspective) depending on which IPsec tunnel gets used.

IP Address
The alternative IP address to negotiate.

Mask

The alternative IP mask to negotiate.

Virtual IP Request
Used when the remote peer is a Cisco device using MODECFG to assign a specific IP address to this router during SA setup negotiations. This is commonly seen in Remote Access (RA) type VPNs and EasyVPN solutions. The mode to use will depend on the configuration of the Cisco, seek advice from the Cisco administrator to determine which mode to use.

XAuth ID
Extended Authentication ID for use with Cisco XAUTH.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eroute	n	debug	on, off	Enable IKE tracing
eroute	n	neglocip	IP Address	Negotiate a different IP address and Mask
eroute	n	neglocmsk	IP Mask	Negotiate a different IP address and Mask
eroute	n	vip	0,1,2,3	Virtual IP address
eroute	n	xauthid	String	XAuth ID

Advanced

IPsec mode
Selects the IPsec encapsulation type to use on the IPsec tunnel. In Tunnel mode, the entire IP packet (header and payload) is encrypted. In Transport mode, only the IP payload is encrypted.

Use algorithm AH authentication on this tunnel
The AH authentication algorithm to use with this IPsec tunnel. The options are:

- No (None)
- MD5
- SHA1

Use algorithm compression on this tunnel
The compression algorithm to use with this IPsec tunnel. The options are:

- No (None)
- DEFLATE

Delete SAs when this tunnel is down
When selected, all SAs associated with the IPsec tunnel are deleted when the tunnel goes out of service.

Delete SAs when router is not a VRRP master
When selected, at least one Ethernet interface must be set as VRRP Master before the router can create SAs. If the router switches away from VRRP Master state, the SAs will be deleted. When the router switches back to VRRP Master state, the SAs will be created automatically.

Go out of service if automatic establishment fails
The router will take the IPsec tunnel out of service if the automatic establishment fails rather than continually retrying.

Go out of service after n consecutive auto-negotiation failures
The router will take the IPsec tunnel out of service if the auto-negotiation fails for the specified consecutive number of times rather than continually retrying.

This tunnel can only use apn
When enabled, this parameter allows you to choose between using the main APN or the backup APN, as defined in the ***Configuration – Network > Serial > W-WAN Port*** page.

Link tunnel with interface with x,y
When enabled, this parameter can be set so that the IPsec tunnel will only match packets using the specified interface. When this parameter is enabled, the route will take outgoing packets going through this IPsec tunnel and recheck to see if the resultant packet also goes through a tunnel.
If the inner tunnel is an IPsec tunnel (i.e. needs IKE), you can get the inner IKE to use the correct source address (matching the outer tunnel selectors) by enabling the **Use secondary IP address** parameter and the inner IKE will use the IP address configured in the **Secondary IP address** parameter on the ***Configuration – Network > Advanced Network Settings*** page.

Inhibit this IPsec tunnel when IPsec tunnels n are up
This is a list of IPsec tunnels that can inhibit this IPsec tunnel from being used as long as they are up. If this IPsec tunnel has been allowed to come up, and the IPsec tunnel that inhibits it comes back up, this IPsec is taken down and any SAs that may have existed are removed. As soon as an inhibiting IPsec tunnel goes down, the router will check to see if the inhibited IPsec tunnel can now create SAs.

Inhibit this IPsec tunnel unless IPsec tunnel n is up
This IPsec tunnel will be inhibited unless specified IPsec tunnel is also up.

IKE negotiation source IP address is taken from the
This defines which IP address IKE uses as the source IP address during the negotiation.

Interface
Use the IP address of the interface over which the IKE packets will be transmitted.

Secondary IP address
Use the IP address configured in the **Secondary IP address** parameter on the ***Configuration – Network > Advanced Network Settings*** page.

Interface x,y
Use the IP address of the specified interface.

Tunnel this IPsec tunnel inside another IPsec tunnel
It is possible to tunnel packets from an IPsec tunnel within a second (or more) tunnel. When this parameter is enabled.

NAT-Traversal Keepalive timer s seconds
Sets the interval period, in seconds, that the router will use to send regular packets to a NAT device in order to prevent the NAT table entry from expiring.

Allow protocol IP protocol(s) in this tunnel
This restricts the type of IP packets that will be tunnelled through the IPsec tunnel. The options are:

- All
- TCP
- UDP
- GRE

IP packets with ToS values n must use this tunnel
Packets with matching ToS fields will only be tunnelled through this IPsec tunnel and no others. The usual traffic selector matching still takes place as normal. Packets that don't have matching ToS values will get tunnelled as normal.
The ToS values should be entered as a comma separated list. E.g. 2,4

Only tunnel IP packets with
This restricts the IP packets that will be tunnelled to those with matching TCP/UDP port numbers.

local TCP/UDP port n
Allow IP packets with matching source TCP/UDP ports to be tunnelled.

remote TCP/UDP port n
Allow IP packets with matching destination TCP/UDP ports to be tunnelled.

local TCP/UDP port in the range of n1 to n2
Allow IP packets with source TCP/UDP ports in the specified range to be tunnelled. This is only available when IKEv2 is used

remote TCP/UDP port in the range of n1 to n2
Allow IP packets with destination TCP/UDP ports in the specified range to be tunnelled. This is only available when IKEv2 is used

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eroute	n	mode	tunnel, transport	IPsec Mode
eroute	n	ahauth	off, md5, sha1	Use a AH authentication on this tunnel
eroute	n	ipcompalg	off, deflate	Use c compression on this tunnel
eroute	n	oosdelsa	on, off	Delete SAs when this tunnel is down
eroute	n	ifvrrpmaster	on, off	Delete SAs when router is not a VRRP master
eroute	n	nosaoos	on, off	Go out of service if automatic establishment fails
eroute	n	nosadeactcnt	Integer	Go out of service after n consecutive auto-negotiation failures
eroute	n	check_apnbu	on, off	This tunnel can only use apn
eroute	n	apnbu	0 = Main APN 1 = Backup APN	This tunnel can only use apn
eroute	n	ifent	blank, ETH, PPP	Link tunnel with interface with x,y x = Interface type
eroute	n	ifadd	Integer	Link tunnel with interface with x,y y = Interface number
eroute	n	inhibitno	Comma separated	Inhibit this IPsec tunnel when

Entity	Instance	Parameter	Values	Equivalent Web Parameter
			list of Integers	IPsec tunnels n are up
eroute	n	requireno	Integer	Inhibit this IPsec tunnel unless IPsec tunnel n is up
eroute	n	usesecip	on, off	IKE negotiation source IP address is taken from the Secondary IP Address
eroute	n	ipent	blank, ETH, PPP	IKE negotiation source IP address is taken from the Interface x,y x = Interface type
eroute	n	ipadd	Integer	IKE negotiation source IP address is taken from the Interface x,y y = Interface number
eroute	n	intunnel	on, off	Tunnel this IPsec tunnel inside another IPsec tunnel
eroute	n	natkaint	Integer	NAT-Traversal Keepalive timer s seconds
eroute	n	proto	off, tcp, udp, gre	Allow protocol IP protocol(s) in this tunnel
eroute	n	toslist	Comma separated list of Integers	IP packets with ToS values n must use this tunnel
eroute	n	locport	0 - 65535	Only tunnel IP packets with local TCP/UDP port
eroute	n	remport	0 - 65535	Only tunnel IP packets with remote TCP/UDP port
eroute	n	locfirstport	0 - 65535	Only tunnel IP packets with local TCP/UDP port in the range of n1 to n2
eroute	n	loclastport	0 - 65535	Only tunnel IP packets with local TCP/UDP port in the range of n1 to n2
eroute	n	remfirstport	0 - 65535	Only tunnel IP packets with remote TCP/UDP port in the range of n1 to n2
eroute	n	remlastport	0 - 65535	Only tunnel IP packets with remote TCP/UDP port in the range of n1 to n2

Setting up IPsec Tunnels for Multiple Users

For small numbers of users it is usual to set up an individual eroute for each user. However, to ease configuration where large numbers of users are required, the "*" character can be used as a wildcard to match multiple user IDs. For example, setting the **Peer ID** parameter to "Digi*" would match all remote units having an **Our ID** parameter starting with "Digi", e.g. Digi01, Digi02, etc.

Example

To setup multiple users in this way, first set up the **Our ID** parameter on the host unit to a suitable name, e.g. “Host1”. Then set the **Peer ID** parameter to “Remote*” for example. In addition, an entry would be made in the user table with “Remote*” for the **Username** and a suitable **Password** value, e.g. “mysecret”.

Each of the remote units that required access to the host would then have to be configured with an **Our ID** parameter of “Remote01”, “Remote02”, etc. and each would have to have an entry in their user table for User Host1 along with its password (i.e. the pre-shared key).

Host Router

Peer ID:	Remote*
Our ID:	Host1
Username:	Remote*
Password:	mysecret

Remote Router 1

Peer ID:	Host1
Our ID:	Remote01
Username:	Host1
Password:	mysecret

Remote Router 2

Peer ID:	Host1
Our ID:	Remote02
Username:	Host1
Password:	mysecret

Remote Router 3

Peer ID:	Host1
Our ID:	Remote03
Username:	Host1
Password:	mysecret

IPsec Default Action

Configuration – Network > Virtual Private Network (VPN) > IPsec > IPsec Default Action

Like a normal IP routing set-up, IPSec Tunnels have a default configuration that is applied if no specific tunnel can be found. This is useful when, for instance, you wish to have a number of remote users connect via a secure channel (perhaps to access company financial information) but also still allow general remote access to other specific servers on your network or the Internet.

When a packet is received which does not match any IPsec tunnel
How the router will respond if a packet is received when there is no SA.
If "Drop the packet" is selected then only packets that match a specified IPsec tunnel will be routed, all other data will be discarded. This has the effect of enforcing a secure connection to all devices behind the router.
If "Pass the packet" is selected then packets that match an IPsec tunnel will be decrypted and authenticated (depending on the IPsec tunnel's configuration) but data that does not match will also be allowed to pass.

When a packet is to be transmitted which does not match any IPsec tunnel
How the router will respond if a packet is transmitted when there is no SA.
If "Drop the packet" is selected then only packets that match a specified IPsec tunnel will be routed, all other data will be discarded.
If "Pass the packet" is selected then data that matches an IPsec tunnel will be encrypted and authenticated (depending on the IPsec tunnel configuration) but data that does not match will also be allowed to pass.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
def_eroute	0	nosain	drop, pass	When a packet is received which does not match any IPsec tunnel
def_eroute	0	nosaout	drop, pass	When a packet is to be transmitted which does not match any IPsec tunnel

IPsec Groups

Configuration – Network > Virtual Private Network (VPN) > IPsec > IPsec Groups

This mode of operation can be used when the router is terminating tunnels to a large number of remote devices e.g. when being used as a VPN Concentrator. To keep the size of the configuration file in the router small and also to maintain ease of configuration, only the information that is used for all tunnels is stored on the router. All other information that is site specific is stored in a MySQL database. This means the number of sites that can be configured is limited only by the SQL database size and performance. This will be literally millions of sites depending upon the operating system and hardware of the MySQL PC. The number of sites that can be connected to concurrently are much smaller and limited by the model of the router.

Basic Concept

The router with the IPsec Group/MySQL configuration will be the VPN Concentrator. The remote sites will normally not require an IPsec group configuration as they will normally only need to connect to a single peer, the VPN Concentrator. The VPN Concentrator will normally need only a single IPsec group configured. The local and remote subnet parameters need to be set up wide enough to encompass all the local and remote networks. The VPN Concentrator can act as an initiator and/or a responder. In situations where there are more remote sites than the Digi can support concurrent sessions, it will normally be necessary for the VPN Concentrator and the remote sites to be both an initiator and a responder. This is so that both the remote sites and the head-end can initiate the IPsec session when required. Note that it is also important to configure the IPsec tunnels to time out on inactivity to free up sessions for other sites. In the case of the VPN Concentrator acting as an initiator, when it receives a packet that matches the main IPsec tunnel, if no Security Associations already exist it will look up the required parameters in the database. The TransPort will then create a "Dynamic IP Tunnel" containing all the settings from the base IPsec tunnel and all the information retrieved from the database. At this point IKE will create the tunnel (IPsec security associations) as normal. The dynamic IPsec tunnel will continue to exist until all the IPsec Security Associations have been removed. At the point where the maximum supported (or licensed) number of tunnels has been reached by the router, the oldest Dynamic IPsec tunnels (those that have not been used for the longest period of time) and their associated IPsec Security Associations will be dropped to allow new inbound VPNs to connect.

Logic flow - creation of IPSec SAs

VPN Concentrator acting as initiator

The VPN Concentrator will normally act as an initiator when it receives an IP packet for routing with a source address matching the IPsec tunnel local subnet address & mask and a destination address matching the remote subnet address & mask (providing that an IPsec SA does not already exist for this site.)

If an IPsec group is configured to use the matching IPsec tunnel, the router will use a MySQL query to obtain the site specific information in order to create the SA's. The VPN Concentrator will create a SELECT query using the destination IP address of the packet and the mask configured in the IPsec group configuration to determine the remote subnet address. (This means that the remote subnet mask must be the same on all sites using the current IPsec group.) Once the site specific information has been retrieved, the router creates a 'dynamic' IPsec Tunnel which is based upon the base IPSec tunnel configuration plus the site specific information from the MySQL database. The router can then use the completed IPsec tunnel configuration and IKE to create the IPsec SAs. For the pre-shared key, IKE will use the password returned from the MySQL database rather than doing a local look up in the user configuration. Once created, the SAs are linked with the dynamic IPsec tunnel. Replacement SAs are created as the lifetimes start to get low and traffic is still flowing. When all SAs to this remote router are removed, the dynamic IPsec tunnel will also be removed so that IPsec tunnel can then be re-used to create tunnels to other remote sites. When processing outgoing packets, dynamic IPsec Tunnels are searched before base IPsec tunnels. So, if a matching dynamic IPsec tunnel is found, it is used, and the base IPsec tunnel is only matched if no dynamic IPsec tunnel exists. Once the dynamic IPsec tunnel is removed, further outgoing packets will match the base IPsec tunnel and the process is repeated.

VPN Concentrator acting as a responder to a session initiated from the remote site

When a remote site needs to create an IPsec SA with the VPN Concentrator it will send an IKE request to the VPN Concentrator. The VPN Concentrator needs to be able to confirm that the remote device is authorised to create an IPsec tunnel. The remote site will supply its ID to the host during the IKE negotiations. The VPN Concentrator will use this ID and look through the IPsec tunnels configured and dynamic IPsec tunnels to see if the supplied ID matches the configured Peer ID (peerid). If a match is found, the MYSQL database is queried to retrieve the information required to complete the negotiation (e.g. pre-shared key/password). If no matching base IPsec tunnel is found, the local user configuration is used to locate the password, and a normally configured IPsec tunnel must also exist. Once the information is retrieved from the MySQL database, IKE negotiations continue and the created IPsec SAs will be associated with the dynamic IPsec tunnel. As long as the dynamic IPsec tunnel exists, it behaves just like a normal IPsec tunnel. i.e. SAs are replaced/removed as required.

If errors are received from the MySQL database, or not enough fields are returned, the dynamic IPsec tunnel is removed, and IKE negotiations in progress will be terminated. There are a limited number of dynamic IPsec tunnel. If the number of free dynamic IPsec tunnel is less than 10% of the total number of dynamic IPsec tunnel, the Digi router will periodically remove the oldest dynamic IPsec tunnel. This is done to ensure that there will always be some free dynamic IPsec tunnel available for incoming connections from remote routers. It is possible to view the current dynamic tunnels that exist using the WEB server, browse to ***Management - Connections > Virtual Private Networking (VPN) > IPsec***. The table will indicate the base IPsec tunnel and the Remote Peer ID in the status display to help identify which remote sites are currently connected.

Preliminary IP Tunnel configuration

The IPsec tunnel configuration ***Configuration – Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec n*** differs from a normal configuration in the following ways:

- Peer IP/hostname: Because the peer IP address to each peer is unknown and is retrieved from the database, this field is left empty.
- Bakpeerip (CLI only): Because the peer IP address to each peer is unknown and is retrieved from the database, this field is left empty.
- Peer ID: When the host Digi is acting as a responder during IKE negotiations, the router uses the ID supplied by the remote to decide whether or not the MySQL database should be interrogated. So that the Digi can make this decision, the remote router must supply an ID that matches the peerid configured into the IPsec tunnel. Wildcard matching is supported which means that the peerid may contain '*' and '?' characters. If only one IPsec tunnel is configured, the peerid field may contain a '*', indicating that all remote IDs result in a MySQL look up.
- Local subnet IP address / Local subnet mask: Configured as usual.
- Remote subnet IP address / Remote subnet mask: These fields should be configured in such a way that packets to ALL remote sites fall within the configured subnet. e.g. if there are two sites with remote subnets 192.168.0.0/24, and 192.168.1.0/24 respectively, a valid configuration for the host would be 192.168.0.0/23 so that packets to both remote sites match.

All other fields should be configured as usual. It is possible to set up other IPsec groups linked with other IPsec tunnels. This would be done if there is a second group of remote sites that have a different set of local and remote subnets, or perhaps different encryption requirements. The only real requirement is that this second group uses peer IDs that do not match up with those in use by the first IPsec group.

IPsec Group configuration

This configuration holds information relating to the MySQL database, and the names of the fields where the information is held. This configuration is also used to identify which IPsec tunnels are used to create dynamic IPsec tunnels.

Example MySQL schema

```
mysql> describe eroutes;
+-----------+-------------+------+-----+---------+-------+
| Field     | Type        | Null | Key | Default | Extra |
+-----------+-------------+------+-----+---------+-------+
| peerip    | varchar(20) | YES  |     | NULL    |       |
| bakpeerip | varchar(20) | YES  |     | NULL    |       |
| peerid    | varchar(20) | NO   | PRI |         |       |
| password  | varchar(20) | YES  |     | NULL    |       |
| ourid     | varchar(20) | YES  |     | NULL    |       |
| remip     | varchar(20) | YES  | UNI | NULL    |       |
| remmsk    | varchar(20) | YES  |     | NULL    |       |
+-----------+-------------+------+-----+---------+-------+
7 rows in set (0.01 sec)
```

Link this IPsec group with IPsec Tunnel
The base IPsec tunnel number. This parameter allows the router to see that an IPsec tunnel should use the group configuration to retrieve dynamic information from the database.

Remote mask to use for tunnels
This parameter is used in the SQL SELECT query in conjunction with the destination IP address of packets to be tunnelled from the host to the remote peer to identify the correct record to select from the MySQL database.

MySQL Server IP Address or Hostname
The IP address or hostname of the MySQL Server.

MySQL Server Port
The port that the MySQL Server is listening on.

Username
The username to use when logging into the MySQL Server.

Password / Confirm Password
The password to use when logging into the MySQL Server.

Database name
The name of the database to connect to.

Database table

The name of the table when the remote site information is stored.

Remote subnet IP
The name of the field in the table where the 'remip' data is stored.

Remote subnet Mask
The name of the field in the table where the 'remmsk' data is stored.

Peer IP Address
The name of the field in the table where the 'peerip' data is stored.

Backup Peer IP Address
The name of the field in the table where the 'bakpeerip" data is stored.

Peer ID
The name of the field in the table where the 'peerid' data is stored.

Our ID
The name of the field in the table where the 'ourid' data is stored.

Password
The name of the field in the table where the password to use in IKE negotiations is stored.

Note:
The default MySQL field names match the matching IPsec tunnel configuration parameter name. The default field name for the 'password' field is 'password'.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
egroup	n	eroute	Integer	Link this IPsec group with IPsec Tunnel
egroup	n	remmsk	IP Mask	Remote mask to use for tunnels
egroup	n	dbhost	IP Address or Hostname	MySQL Server IP Address or Hostname
egroup	n	dbport	0 - 65535	MySQL Server Port
egroup	n	dbuser	String	Username
egroup	n	dbpwd	String	Password / Confirm Password
egroup	n	dbname	String	Database name
egroup	n	dbtable	String	Database table
egroup	n	fremip	String	Remote subnet IP
egroup	n	fremmsk	String	Remote subnet Mask
egroup	n	fpeerip	String	Peer IP Address
egroup	n	fbakpeerip	IP Address	Backup Peer IP Address
egroup	n	fpeerid	String	Peer ID
egroup	n	fourid	String	Our ID
egroup	n	fpwd	String	Password

Dead Peer Detection

Configuration – Network > Virtual Private Network (VPN) > IPsec > Dead Peer Detection

When Dead Peer Detection (DPD) is enabled on an IPsec tunnel, the router will send an IKE DPD request at regular intervals. If no response is received to the DPD request, the IPsec tunnel is considered as suspect and the requests are sent at a shorter interval until either the maximum number of outstanding requests allowed is reached or a response is received. If no response is received to the configured maximum requests, the IPSec tunnels are closed.

Note:
IKE DPD requests require that an IKE SA is present. If one is not present, the DPD request will fail.

To help ensure that an IKE SA exists with a lifetime at least as great as the IPsec lifetime, the router creates new IKE SAs whenever the IPsec SA lifetime exceeds the lifetime of an existing IKE SA and attempts to negotiate a lifetime for the IKE SA that is 60 seconds longer than the desired lifetime of the IPsec SA.

Mark the IPsec tunnel as suspect if there is no traffic for n seconds
The period of time of inactivity on a tunnel before it is deemed to be suspect, i.e. if there is no activity on a healthy link for the time period defined, then the tunnel is them deemed to be suspect.

Send a DPD request on a healthy link every n seconds
The interval at which DPD requests are sent on an IPsec tunnel that is deemed to be healthy. A healthy link is one with traffic.

Send a DPD request on a suspect link every n seconds
The interval at which DPD requests are sent on an IPsec tunnel that is deemed to be suspect. A suspect link is one where there has been no traffic for a specified period of time.

Close the IPsec tunnels after no response for n DPD requests
The maximum number of DPD requests that will be sent without receiving a response before the IPsec tunnels are closed.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dpd	0	inact	Integer	Mark the IPsec tunnel as suspect if there is no traffic for n seconds
dpd	0	okint	Integer	Send a DPD request on a healthy link every n seconds
dpd	0	failint	Integer	Send a DPD request on a suspect link every n seconds
dpd	0	maxfail	Integer	Close the IPsec tunnels after no response for n DPD requests

IKE

Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE

The ***Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE*** folder opens to list configuration pages for ***IKE 0*** and ***IKE 1*** with a separate page for ***IKE Responder***. The IKE 0 instance can be used as an IKE "initiator" or as an IKE "responder" whereas IKE 1 can only be used as an initiator. The ***IKE 0*** and ***IKE 1*** pages are therefore used to set up the IKE 0 and IKE 1 initiator parameters as required. The ***IKE Responder*** page is used to set up the responder parameters for IKE 0.

IKE Debug

Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE> IKE Debug

Enable IKE Debug
Enables IKE debugging to be displayed on the debug port.

Debug Level
Sets the level of IKE debugging. The options are:

- Low
- Medium
- High
- Very High

Debug IP Address Filter
This parameter is used to filter out IKE packets with particular source or destination IP addresses. The format of this parameter is a comma-separated list of IP addresses. For example, you may wish to exclude the capture of IKE traffic from IP hosts 10.1.2.3 and 10.2.2.2. This can be done by entering "10.1.2.3,10.2.2.2" for this parameter. Conversely, you may wish to only capture traffic to and from particular IP hosts. To do this, use a tilde (~) symbol before the list of IP addresses. For example, to only capture packets to and from IP host 192.168.47.1, enter "~192.168.47.1" for this parameter.

Forward debug to port
When enabled, the IKE debug is sent to debug serial port.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike	0	deblevel	0 = Off 1 = Low 2 = Medium 3 = High 4 = Very High	Debug Level
ike	0	ipaddfilt	Comma separated list of IP addresses	Debug IP Address Filter

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike	0	debug	on, off	Forward debug to port

IKE n

Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE> IKE n

Use the following settings for negotiation
Defines the settings used during the IKE negotiation

Encryption
Defines the encryption algorithm used. The options are:

- None
- DES
- 3DES
- AES (128 bit keys)
- AES (192 bit keys)
- AES (256 bit keys)

Authentication
Defines the authentication algorithm used. The options are:

- None
- MD5
- SHA1

Mode
Defines the negotiation mode. The options are:

- Main
- Aggressive

Historically, fixed IP addresses have been used in setting up IPSec tunnels. Today it is more common, particularly with Internet ISPs, to dynamically allocate the user a temporary IP address as part of the process of connecting to the Internet. In this case, the source IP address of the party trying to initiate the tunnel is variable and cannot be pre-configured.
In Main mode (i.e. non-aggressive), the source IP address must be known i.e. this mode can only be used over the Internet if the ISP provides a fixed IP address to the user or you are using X.509 certificates.
Aggressive mode was developed to allow the host to identify a remote unit (initiator) from an ID string rather than from its IP address. This means that it can be used over the Internet via an ISP that dynamically allocates IP addresses. It also has two other noticeable differences from main mode. Firstly, it uses fewer messages to complete the phase 1 exchange (3 compared to 5) and so will execute a little more quickly, particularly on networks with large turn-around delays such as GPRS. Secondly, as more information is sent unencrypted during the exchange, it is potentially less secure than a normal mode exchange.

Note:
Main mode can be used without knowing the remote unit's IP address when using

certificates. This is because the ID of the remote unit (it's public key) can be retrieved from the certificate file.

MODP Group for Phase 1
Sets the key length used in the IKE Diffie-Hellman exchange to768 bits (group 1) or 1024 bits (group 2). Normally this option is set to group 1 and this is sufficient for normal use. For particularly sensitive applications, you can improve security by selecting group 2 to enable a 1024 bit key length. Note however that this will slow down the process of generating the phase 1 session keys (typically from 1-2 seconds for group 1), to 4-5 seconds.

MODP Group for Phase 2
Sets the minimum width of the numeric field used in the calculations for phase 2 of the security exchange.
With "No PFS" (Perfect Forwarding Security) selected, the data transferred during phase 1 can be reused to generate the keys for the phase 2 SAs (hence speeding up connections). However, in doing this it is possible (though very unlikely), that if the phase 1 keys were compromised (i.e. discovered by a third party), the phase 2 keys might be more easily compromised.
Enabling group 1 (768) or 2 (1024) or 3 (1536), IPSec MODP forces the key calculation for phase 2 to use new data that has no relationship to the phase 1 data and initiates a second Diffie-Hellman exchange. This provides an even greater level of security but of course can take longer to complete.

Renegotiate after h hrs m mins s secs
Determines how long the initial IKE Security Association will stay in force. When it expires any attempt to send packets to the remote system will result in IKE attempting to establish a new SA.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike	n	encalg	des, 3des, aes	Encryption
ike	n	keybits	0, 128, 192, 256	Encryption (AES Key length)
ike	n	authalg	md5, sha1	Authentication
ike	n	aggressive	on, off	Mode
ike	n	ikegroup	1, 2, 5	MODP Group for Phase 1
ike	n	ipsecgroup	1, 2, 5	MODP Group for Phase 2
ike	n	ltime	1 - 28800	Renegotiate after h hrs m mins s secs This CLI value is entered in seconds only.

Advanced

Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE> IKE n> Advanced

Retransmit a frame if no response after n seconds
The amount of time in seconds that IKE will wait for a response from the remote unit before transmitting the negotiation frame.

Stop IKE negotiation after n retransmissions
The maximum number of times that IKE will retransmit a negotiation frame as part of the exchange before failing.

Stop IKE negotiation if no packet received for n seconds
The period of time in seconds after which the unit will stop the IKE negotiation when no response to a negotiation packet has been received.

Enable Dead Peer Detection
Enables Dead Peer Detection. For more information, refer to the ***Configuration – Network > IPsec > Dead Peer Detection (DPD)*** page.

Enable NAT-Traversal
Enables support for NAT Traversal within IKE/IPsec. When one end of an IPsec tunnel is behind a NAT box, some form of NAT traversal may be required before the IPsec tunnel can pass packets. Turning NAT Traversal on enables the IKE protocol to discover whether or not one or both ends of a tunnel is behind a NAT box, and implements a standard NAT traversal protocol if NAT is not being performed.
The version of NAT traversal supported is that described in the IETF draft 'draft-ietf-ipsec-nat-t-ike-03.txt'.

Send INITIAL-CONTACT notifications
Enables INITIAL-CONTACT notifications to be sent.

Retain phase 1 SA after failed phase 2 negotiation
Normally IKE functionality is to remove the phase 1 SA if the phase 2 negotiation fails. Enabling this parameter will cause the router to retain the existing phase 1 SA and retry the phase 2 again.

RSA private key file
The name of a X.509 certificate file holding the router's private part of the public/private key pair used in certificate exchanges. See 'X.509 Certificates' in the 'IPsec and VPNs' section for further explanation.

SA Removal Mode
Determines how IPsec and IKE SAs are removed.
'Normal' operation will not delete the IKE SA when all the IPsec SAs that were created by it are removed and will not remove IPsec SAs when the IKE SA that was used to create them is deleted.
'Remove IKE SA when last IPSec SA removed' will delete the IKE SA when all the IPsec SAs that it created to a particular peer are removed.
'Remove IPSec SAs when IKE SA removed' will delete all IPSec SAs that have been created by the IKE SA that has been removed.
'Both' will remove IPSec SAs when their IKE SA is deleted, and delete IKE SAs when their IPSec SAs are removed.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike	n	retranint	0 - 255	Retransmit a frame if no response after n seconds
ike	n	retran	0 - 9	Stop IKE negotiation after n retransmissions
ike	n	inactto	0 - 255	Stop IKE negotiation if no packet received for n seconds

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike	n	dpd	on, off	Enable Dead Peer Detection
ike	n	natt	on, off	Enable NAT-Traversal
ike	n	initialcontact	on, off	Send INITIAL-CONTACT notifications
ike	n	keepph1	on, off	Retain phase 1 SA after failed phase 2 negotiation
ike	n	privrsakey	Filename	RSA private key file
ike	n	delmode	0 = Normal 1 = Remove IKE SA when last IPsec SA removed 2 = Remove IPsec SAs when IKE SA remove 3 = Both	SA Removal Mode
ike	n	openswan	on, off	None. This enables support for Openswan IKE implementations.

IKE Responder

Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE> IKE Responder

This page displays the various parameters for IKE 0 when used in Responder mode.

Enable IKE Responder
Allows the router to respond to incoming IKE requests.

Accept IKE Requests with
Defines the settings that the router will accept during the negotiation

Encryption
The acceptable encryption algorithms.

Authentication
The acceptable authentication algorithms.

MODP Group between x and y
The acceptable range for MODP group.

Renegotiate after h hrs m mins s secs
Determines how long the initial IKE Security Association will stay in force. When it expires any attempt to send packets to the remote system will result in IKE attempting to establish a new SA.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike	0	noresp	on, off	Enable IKE Responder

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike	0	rencalgs	des, 3des, aes Multiple algorithms can specified in a comma separated list	Encryption
ike	0	keybits	0, 128, 192, 256	Encryption (Minimum AES Key length)
ike	0	rauthalgs	md5, sha1 Multiple algorithms can specified in a comma separated list	Authentication
ike	0	rdhmingroup	1, 2, 5	MODP Group between x and y
ike	0	rdhmaxgroup	1, 2, 5	MODP Group between x and y
ike	0	ltime	1 - 28800	Renegotiate after h hrs m mins s secs This CLI value is entered in seconds only.

Advanced

Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE> IKE Responder> Advanced

Stop IKE negotiation if no packet received for n seconds
The period of time in seconds after which the unit will stop the IKE negotiation when no response to a negotiation packet has been received.

Enable NAT-Traversal
Enables support for NAT Traversal within IKE/IPsec. When one end of an IPsec tunnel is behind a NAT box, some form of NAT traversal may be required before the IPsec tunnel can pass packets. Turning NAT Traversal on enables the IKE protocol to discover whether or not one or both ends of a tunnel is behind a NAT box, and implements a standard NAT traversal protocol if NAT is not being performed.
The version of NAT traversal supported is that described in the IETF draft 'draft-ietf-ipsec-nat-t-ike-03.txt'.

Send INITIAL-CONTACT notifications
Enables INITIAL-CONTACT notifications to be sent.

Send RESPONDER-LIFETIME notifications
Enables RESPONDER-LIFETIME notifications sent to the initiator. If an initiator requests an IKE lifetime that is greater than the responder, a notification will be sent and the initiator should reduce its lifetime value accordingly.

Retain phase 1 SA after failed phase 2 negotiation
The name of a X.509 certificate file holding the router's private part of the public/private key pair used in certificate exchanges. See 'X.509 Certificates' in the 'IPsec and VPNs' section for further explanation.

RSA private key file

The name of a X.509 certificate file holding the router's private part of the public/private key pair used in certificate exchanges. See 'X.509 Certificates' in the 'IPsec and VPNs' section for further explanation.

SA Removal Mode
Determines how IPsec and IKE SAs are removed.
'Normal' operation will not delete the IKE SA when all the IPsec SAs that were created by it are removed and will not remove IPsec SAs when the IKE SA that was used to create them is deleted.
'Remove IKE SA when last IPSec SA removed' will delete the IKE SA when all the IPsec SAs that it created to a particular peer are removed.
'Remove IPSec SAs when IKE SA removed' will delete all IPSec SAs that have been created by the IKE SA that has been removed.
'Both' will remove IPSec SAs when their IKE SA is deleted, and delete IKE SAs when their IPSec SAs are removed.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike	0	inactto	0 – 255	Stop IKE negotiation if no packet received for n seconds
ike	0	natt	on, off	Enable NAT-Traversal
ike	0	initialcontact	on, off	Send INITIAL-CONTACT notifications
ike	0	respltime	on, off	Send RESPONDER-LIFETIME notifications
ike	0	keepph1	on, off	Retain phase 1 SA after failed phase 2 negotiation
ike	0	privrsakey	Filename	RSA private key file
ike	0	delmode	0 = Normal 1 = Remove IKE SA when last IPsec SA removed 2 = Remove IPsec SAs when IKE SA remove 3 = Both	SA Removal Mode

MODECFG Static NAT mappings

Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKE> MODECFG Static NAT mappings

MODECFG is an extra stage built into IKE negotiations that fits between IKE phase 1 and IKE phase 2, and is used to perform operations such as extended authentication (XAUTH) and requesting an IP address from the host. This IP address becomes the source address to use when sending packets through the tunnel from the remote to the host. This mode of operation (receiving one IP address from the remote host) is called "client" mode. Another mode, called "network" mode, allows the unit to send packets with a range of source addresses through the tunnel.

If the unit receives packets from a local interface that need to be routed through the tunnel, it performs address translation so that the source address matches the assigned IP address before encrypting using the negotiated SA. Some state information is retained so that packets coming in the opposite direction with matching addresses/ports can have their destination address set to the source address of the original packet (in the same way as standard NAT).

If the remote end of the tunnel is to be able to access units connected to the local interface, the unit that has been assigned the virtual IP address needs to have some static NAT entries set up. When a packet is received through the tunnel, the unit will first look up existing NAT entries, followed by static NAT entries to see if the destination address/port should be modified, and forwards the packet to the new address. If a static NAT mapping is found, the unit creates a dynamic NAT entry that will be used for the duration of the connection. If no dynamic or stateful entry is found, the packet is directed to the local protocol handlers.

External Port
The lowest destination port number to be matched if the packet is to be redirected.

Forward to Internal IP Address
An IP address to which packets containing the specified destination port number are to be redirected.

Forward to Internal Port
A port number to which packets containing the specified destination port number are to be redirected.

Port Range Count
The number of ports to be matched.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
tunsnat	n	minport	0 - 65535	External Port
tunsnat	n	maxport	0 – 65535	Port Range Count
tunsnat	n	ipaddr	IP Address	Forward to Internal IP Address
tunsnat	n	mapport	0 - 65535	Forward to Internal Port

IKEv2

Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKEv2

When IKE Version 2 is supported, it is possible to specify whether the IKEv1 or IKEv2 protocol should be used to negotiate IKE SAs. By default, IKEv1 is used and routers which have been upgraded to support IKEv2 will not require any changes to their configuration to continue working with IKEv1.

IKEv2 n

Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKEv2> IKEv2 n

Use the following settings for negotiation
Defines the settings used during the IKEv2 negotiation

Encryption
Defines the encryption algorithm used. The options are:

- None
- DES
- 3DES
- AES (128 bit keys)
- AES (192 bit keys)
- AES (256 bit keys)

Authentication
Defines the authentication algorithm used. The options are:

- None
- MD5
- SHA1

PRF Algorithm
Defines the PRF (Pseudo Random Function) algorithm used. The options are:

- MD5
- SHA1

MODP Group for Phase 1
Sets the key length used in the IKE Diffie-Hellman exchange to768 bits (group 1) or 1024 bits (group 2). Normally this option is set to group 1 and this is sufficient for normal use. For particularly sensitive applications, you can improve security by selecting group 2 to enable a 1024 bit key length. Note however that this will slow down the process of generating the phase 1 session keys (typically from 1-2 seconds for group 1), to 4-5 seconds.

Renegotiate after h hrs m mins s secs
Determines how long the initial IKEv2 Security Association will stay in force. When it expires any attempt to send packets to the remote system will result in IKE attempting to establish a new SA.

Rekey after h hrs m mins s secs
When the time left until expiry for this SA reaches the value specified by this parameter, the IKEv2 SA will be renegotiated, i.e. a new IKEv2 SA is negotiated and the old SA is removed. Any IPSec “child” SAs that were created are retained and become “children” of the new SA.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike2	n	iencalg	des, 3des, aes	Encryption
ike2	n	ienkeybits	128, 192, 256	Encryption (AES Key length)
ike2	n	iauthalg	md5, sha1	Authentication
ike2	n	iprfalg	md5, sha1	PRF Algorithm
ike2	n	idhgroup	1, 2, 5	MODP Group for Phase 1
ike2	n	ltime	1 - 28800	Renegotiate after h hrs m mins s secs This CLI value is entered in seconds

Entity	Instance	Parameter	Values	Equivalent Web Parameter
				only.
ike2	n	rekeyltime	1 - 28800	Rekey after h hrs m mins s secs This CLI value is entered in seconds only.

Advanced

Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKEv2> Advanced

Retransmit a frame if no response after n seconds
The amount of time in seconds that IKEv2 will wait for a response from the remote unit before transmitting the negotiation frame.

Stop IKE negotiation after n retransmissions
The maximum number of times that IKEv2 will retransmit a negotiation frame as part of the exchange before failing.

Stop IKE negotiation if no packet received for n seconds
The period of time in seconds after which the unit will stop the IKE v2 negotiation when no response to a negotiation packet has been received.

Enable NAT-Traversal
Enables support for NAT Traversal within IKE/IPsec. When one end of an IPsec tunnel is behind a NAT box, some form of NAT traversal may be required before the IPsec tunnel can pass packets. Turning NAT Traversal on enables the IKE protocol to discover whether or not one or both ends of a tunnel is behind a NAT box, and implements a standard NAT traversal protocol if NAT is not being performed.
The version of NAT traversal supported is that described in the IETF draft 'draft-ietf-ipsec-nat-t-ike-03.txt'.

NAT traversal keep-alive interval n seconds
The interval in seconds in which the NAT Traversal keepalive packets are sent to a NAT device in order to prevent NAT table entry from expiring.

RSA private key file
The name of a X.509 certificate file holding the router's private part of the public/private key pair used in certificate exchanges. See 'X.509 Certificates' in the 'IPsec and VPNs' section for further explanation.

Related CLI Commands

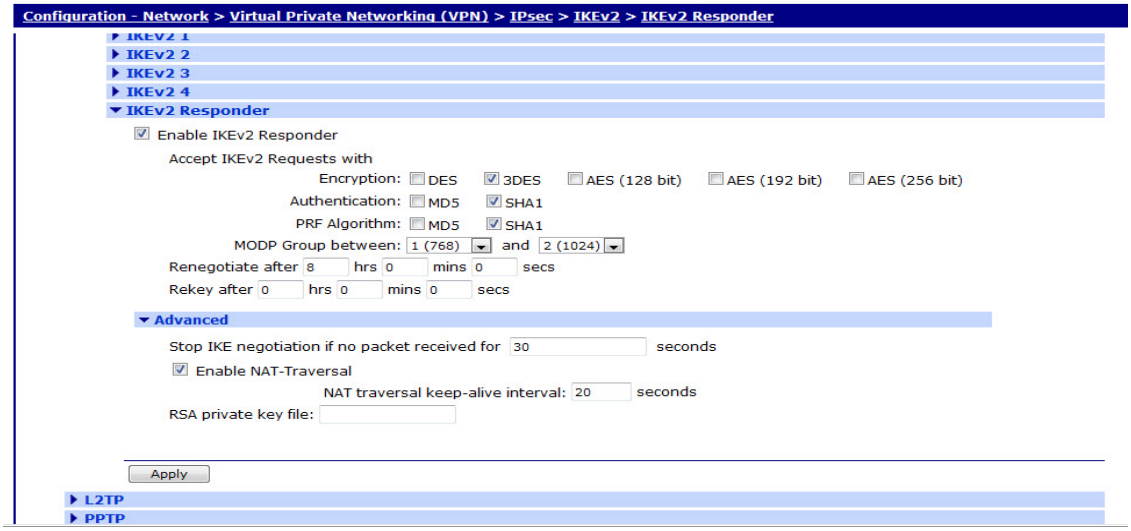
Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike2	n	retranint	0 - 255	Retransmit a frame if no response after n seconds
ike2	n	retran	0 - 9	Stop IKE negotiation after n retransmissions
ike2	n	inactto	0 - 255	Stop IKE negotiation if no packet received for n seconds
ike2	n	natt	on, off	Enable NAT-Traversal
ike2	n	natkaint	Integer	NAT traversal keep-alive interval n seconds

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike2	n	privrsakey	Filename	RSA private key file

IKEv2 Responder

Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKEv2> IKEv2 Responder

This page displays the various parameters for IKEv2 0 when used in Responder mode.


Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKEv2 > IKEv2 Responder
IKEv2 1
IKEv2 2
IKEv2 3
IKEv2 4
IKEv2 Responder
Enable IKEv2 Responder
Accept IKEv2 Requests with
Encryption: DES 3DES AES (128 bit) AES (192 bit) AES (256 bit)
Authentication: MD5 SHA1
PRF Algorithm: MD5 SHA1
MODP Group between: 1 (768) and 2 (1024)
Renegotiate after 8 hrs 0 mins 0 secs
Rekey after 0 hrs 0 mins 0 secs
Advanced
Stop IKE negotiation if no packet received for 30 seconds
Enable NAT-Traversal
NAT traversal keep-alive interval: 20 seconds
RSA private key file:
Apply
L2TP
PPTP

Enable IKEv2 Responder
Allows the router to respond to incoming IKE requests.

Accept IKEv2 Requests with
Defines the settings that the router will accept during the negotiation

Encryption
The acceptable encryption algorithms.

Authentication
The acceptable authentication algorithms.

PRF Algorithm
The acceptable PRF (Pseudo Random Function) algorithms.

MODP Group between x and y
The acceptable range for MODP group.

Renegotiate after h hrs m mins s secs
Determines how long the initial IKE Security Association will stay in force. When it expires any attempt to send packets to the remote system will result in IKE attempting to establish a new SA.

Rekey after h hrs m mins s secs
When the time left until expiry for this SA reaches the value specified by this parameter, the IKEv2 SA will be renegotiated, i.e. a new IKEv2 SA is negotiated and the old SA is removed. Any IPSec “child” SAs that were created are retained and become “children” of the new SA.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike2	0	rencalgs	des, 3des, aes	Encryption
ike2	0	renckeybits	128, 192, 256	Encryption (Minimum AES key length)
ike2	0	rauthalgs	md5, sha1	Authentication
ike2	0	rprfalgs	md5, sha1	PRF Algorithm
ike2	0	rdhmingroup	1, 2, 5	MODP Group between x and y
ike2	0	rdhmaxgroup	1, 2, 5	MODP Group between x and y
ike2	0	ltime	1 – 28800	Renegotiate after h hrs m mins s secs This CLI value is entered in seconds only.
ike2	0	rekeyltime	1 - 28800	Rekey after h hrs m mins s secs This CLI value is entered in seconds only.

Advanced

Configuration - Network > Virtual Private Networking (VPN) > IPsec > IKEv2> IKEv2 Responder> Advanced

Stop IKE negotiation if no packet received for n seconds
The period of time in seconds after which the unit will stop the IKEv2 negotiation when no response to a negotiation packet has been received.

Enable NAT-Traversal
Enables support for NAT Traversal within IKE/IPsec. When one end of an IPsec tunnel is behind a NAT box, some form of NAT traversal may be required before the IPsec tunnel can pass packets. Turning NAT Traversal on enables the IKE protocol to discover whether or not one or both ends of a tunnel is behind a NAT box, and implements a standard NAT traversal protocol if NAT is not being performed.
The version of NAT traversal supported is that described in the IETF draft 'draft-ietf-ipsec-nat-t-ike-03.txt'.

NAT traversal keep-alive interval n seconds
The interval in seconds in which the NAT Traversal keepalive packets are sent to a NAT device in order to prevent NAT table entry from expiring.

RSA private key file
The name of a X.509 certificate file holding the router's private part of the public/private key pair used in certificate exchanges. See 'X.509 Certificates' in the 'IPsec and VPNs' section for further explanation.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike2	0	inactto	0 - 255	Stop IKE negotiation if no packet received for n seconds

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ike2	0	natt	on, off	Enable NAT-Traversal
ike2	0	natkaint	Integer	NAT traversal keep-alive interval n seconds
ike2	0	privrsakey	Filename	RSA private key file

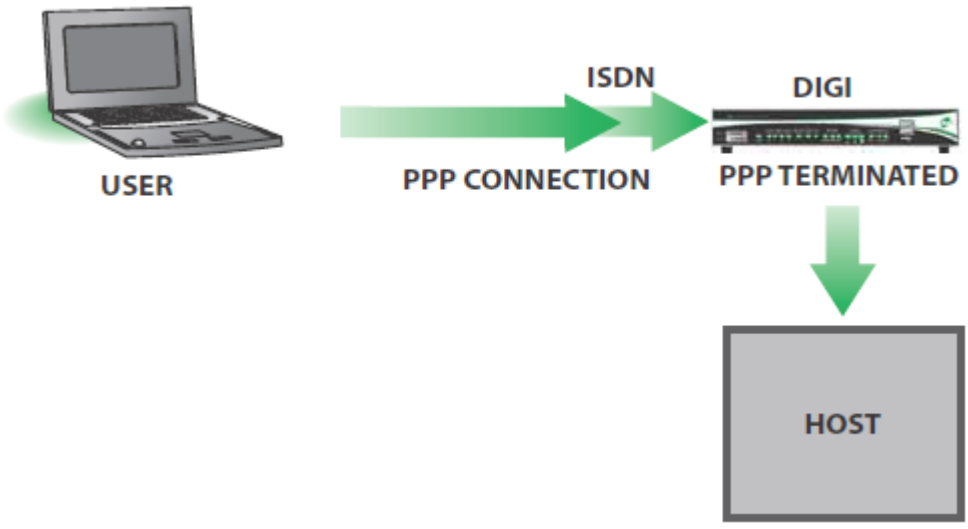
L2TP

Configuration - Network > Virtual Private Networking (VPN) > L2TP

The Layer 2 Tunnelling Protocol (L2TP) provides a means for terminating a logical PPP connection on a device other than the one which terminates the physical connection. Typically, both the physical layer and logical layer PPP connections would be terminated on the same device, a Digi Router for example.



With L2TP answering the call, the router terminates the layer 2 connection only and the PPP frames are passed in an L2TP “tunnel” to another device which terminates the PPP connection. This device is sometimes referred to as a Network Access Server (NAS).



L2TP n

Configuration - Network > Virtual Private Networking (VPN) > L2TP> L2TP n

Act as a listener only

When checked, this checkbox causes the router to NOT actively attempt to establish an L2TP tunnel. In this mode it will only use L2TP if the remote host requests it. When unchecked, the router will actively try to establish an L2TP connection with the remote host.

Enable Server mode
When checked, this checkbox causes the router to act as a L2TP server.

Initiate connections to a.b.c.d
The value in this text box specifies the IP address of the remote host, i.e. the device that will terminate the L2TP connection.

Use a.b.c.d as a backup
It is possible to specify a backup remote L2TP host server using this parameter. The text box contains the IP address of the remote server to use.

Bring this tunnel up All the time / On demand

This parameter only applies to tunnels initiated from this router.

Bring this tunnel down if it is idle for h hrs, m mins, s secs
These radio buttons select whether or not the tunnel is permanently available or not. When set to **On demand**, the tunnel will not activate automatically but will wait until it is triggered by PPP. When set to **On demand** the values in the text boxes determine the timeout after which the L2TP tunnel will closed down after the last L2TP call on that tunnel.

L2TP Window Size
The L2TP window size is selected from this drop down list. Available values are from 1 to 7.

Route UDP packets over interface x,y
These two text boxes specify the interface and its instance number that should be used for L2TP UDP sockets. Specifying these parameters allow the router to raise the interface should it be disconnected.

Source Port Normal / Variable
These radio buttons select the source port for the L2TP tunnel. When set to **Normal** the default port number of 1701 is used. When set to **Variable** a random source port value will be used.

Name
The value in this text box is the name that is used to identify the router during the negotiation phase when establishing an L2TP tunnel.

Authentication Off / Secret
The radio buttons select whether or not to use authentication. This is normally set to **Off** as most host systems require that IPsec be used over L2TP tunnels. If Authentication is set to **On**, authentication is enabled and the **Secret** parameter becomes relevant. The value in the text box contains a passphrase that is shared with the host and which will be used if the remote host requests authentication and **Authentication** is set to **Off** here.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
l2tp	n	listen	OFF,ON	Act as a listener only
l2tp	n	swap_io	OFF,ON	Enable server mode
l2tp	n	remhost	Valid IP address a.b.c.d	Initiate connections to a.b.c.d
l2tp	n	backremhost	Valid IP address	Use a.b.c.d as a backup

Entity	Instance	Parameter	Values	Equivalent Web Parameter
			a.b.c.d	
l2tp	n	aot	OFF,ON	Bring this tunnel up All the time/On demand
l2tp	n	nocallto	0 - 4294967296	Bring this tunnel down if it is idle for h hrs, m mins, s secs
l2tp	n	window	1 – 7 Default = 4	L2TP Window Size
l2tp	n	ll_ent	<blank>, PPP, ETH	Route UDP packets over interface x,y
l2tp	n	ll_add	0 - 2147483647	Route UDP packets over interface x,y
l2tp	n	rnd_srcport	OFF, ON	Source Port
l2tp	n	name	Up to 30 characters	Name
l2tp	n	auth	OFF,ON	Authentication Off/Secret
l2tp	n	secret	Up to 80 characters	Authentication Off/Secret

Advanced

Configuration - Network > Virtual Private Networking (VPN) > L2TP> L2TP n> Advanced

Retransmit interval s milliseconds

The value in this text box specifies the amount of time in milliseconds that the router will wait before retransmitting a Start Control Connection Request (SCCRQ) frame. The default value of 250ms should be changed to a higher value (say 4000ms) if L2TP is running over a GPRS link.

Retransmit count n

When using L2TP over GPRS or satellite networks, the first few packets are sometimes lost. Setting the retransmit count in the text box to a higher value than the default of 5 will increase reliability of the tunnel.

Layer 1 Interface Sync port n / ISDN

These radio buttons select the layer 1 (physical) interface to be used to terminate the L2TP connection. The available options are ISDN or one of the router's synchronous serial ports. When Sync port n is selected, the sync port number is selected from the drop-down list.

Allow this L2TP tunnel to answer incoming ISDN calls

When checked, this checkbox allows the L2TP entity to answer incoming ISDN calls.

MSN

The value in this text box specifies the filter for the ISDN Multiple Subscriber Numbering (MSN). It is blank by default but when the answering facility (above) is enabled, the router will only answer ISDN calls where the trailing digits match this MSN value. For example, setting the MSN value to 123 will prevent the router from answering calls from any calling number that does not end in 123. This parameter is not used when answering is off.

Sub-address
The value in this text box specifies the ISDN sub-address filter to use in conjunction with the ISDN answering function. When answering is set to **On** and there is a valid sub-address in this text box, the router will only answer calls where the trailing digits of the calling sub-address match this sub-address. For example, setting the sub-address value to 123 will prevent the router from answering calls where the sub-address does not end in 123.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
l2tp	n	retxto	0 - 4294967296	Retransmit interval s milliseconds
l2tp	n	retxcnt	0 - 4294967296	Retransmit count
l2tp	n	l1iface	0 – 255	Layer 1 Interface
l2tp	n	ans	OFF,ON	Allow this L2TP tunnel to answer incoming ISDN calls
l2tp	n	msn	Up to 9 digits	MSN
l2tp	n	sub	Up to 17 digits	Sub-address

PPTP

Configuration - Network > Virtual Private Networking (VPN) > PPTP

The Point-to-Point tunnelling protocol (PPTP) is a common way of creating a VPN tunnel to a Microsoft Windows™ server.

PPTP works by ending a regular PPP session to the peer encapsulated by the Generic Routing Encapsulation (GRE) protocol. A second session on TCP port 1723 is used to initiate and manage the GRE session. PPTP connections are authenticated with Microsoft MSCHAP-v2 or EAP-TLS. VPN traffic is protected by MPPE encryption. PPTP does not work with GPRS/HSDPA mobile operators that assign a private IP address and then apply NAT to the traffic before it leaves their network. This because the server tries to build a tunnel back to the router on port 1723 but fails when the traffic is blocked by the mobile operators' firewall.

PPTP n

Configuration - Network > Virtual Private Networking (VPN) > PPTP > PPTP n

Description
The text string in this text box is a name to aid the identification of the router.

Remote Host a.b.c.d
The value in this text box specifies the IP address of the remote host, i.e. the device that will terminate the PPTP connection.

Use Interface x,y
The interface to be used for the PPTP tunnel is selected from this drop-down list, the text box next to it is for the interface instance. Specifying these parameters allow the router to raise the interface should it be disconnected. The interface options are:

- Auto
- PPP
- Ethernet.

Accept incoming PPTP connections
When checked, this checkbox allow the router to act as a PPTP server and accept incoming VPN connections.

Enable Server mode
When checked, this checkbox causes the router to send call_out call requests to the remote device. In the default state which is unchecked, the router will send a call_in request to the remote device.

Enable Socket mode
When checked, this checkbox enables the use of a Digi proprietary mode whereby PPP packets are sent via the PPTP control socket rather than in GRE packets.

Encrypt control data using SSL version n
When checked, this checkbox causes the router to encrypt the control data using SSL. This is a Digi proprietary function and is not part of standard PPTP. The drop-down list allows the SSL version to be selected. The available options are:

- Use default
- TLSv1 only
- SSLv3 only
- SSLv2 only.

Enable PPTP debug
When checked, this checkbox enables debug tracing.

Related CLI Commands

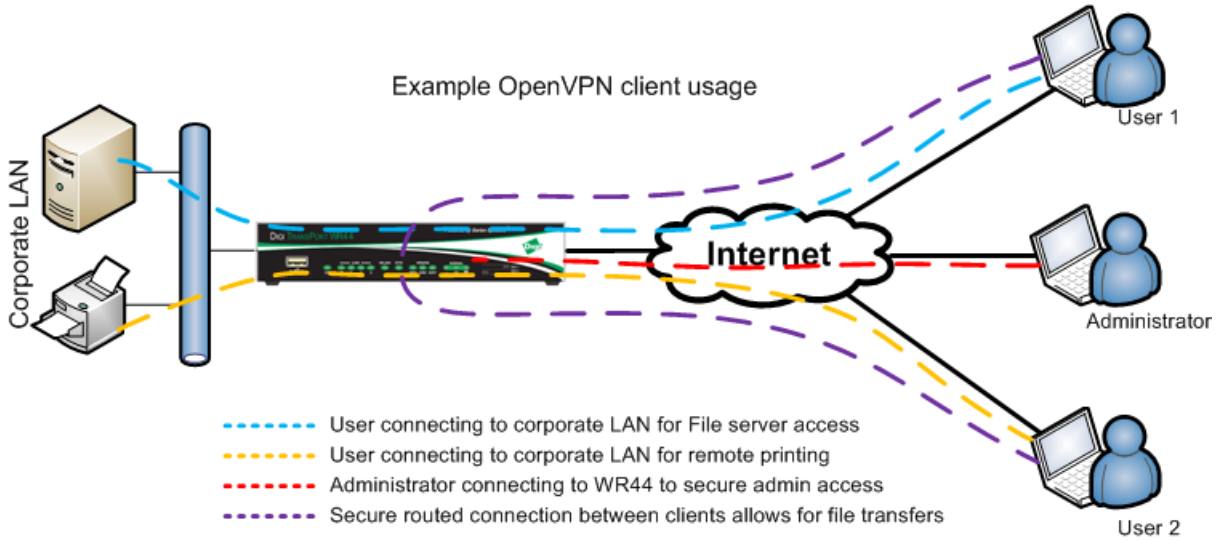
Entity	Instance	Parameter	Values	Equivalent Web Parameter
pptp	0 - 9	name	Up to 30 characters	Description
pptp	0 - 9	remhost	Valid IP address a.b.c.d	Remote Host a.b.c.d
pptp	0 - 9	ll_ent	Blank, PPP, ETH Blank means Auto	Use Interface x,y
pptp	0 - 9	ll_add	0 - 4294967296	Use Interface x,y
pptp	0 - 9	listen	OFF,ON	Accept incoming PPTP connections
pptp	0 - 9	swap_io	OFF,ON	Enable Server mode
pptp	0 - 9	usesock	OFF,ON	Enable Socket mode
pptp	0 - 9	sslver	Blank,SSL,TLS1,SSL3,SSL2 Blank is disabled (default) SSL means use default.	Encrypt control data using SSL version n
pptp	0 - 9	debug	OFF,ON	Enable PPTP debug

OpenVPN

Configuration - Network > Virtual Private Networking (VPN) > OpenVPN

OpenVPN can be used for connecting to the router for secure management as well as access to services on the LAN side of the TransPort router, such as corporate messaging services, file servers and print servers for example.

OpenVPN is a full-featured SSL VPN which implements OSI layer 2 or 3 secure network extension using the industry standard SSL/TLS protocol, supports flexible client authentication methods based on certificates, smart cards, and/or username/password credentials, and allows user or group-specific access control policies using firewall rules applied to the VPN virtual interface. OpenVPN is not a web application proxy and does not operate through a web browser.


Example OpenVPN client usage
Corporate LAN
Internet
User 1
Administrator
User 2
User connecting to corporate LAN for File server access
User connecting to corporate LAN for remote printing
Administrator connecting to WR44 to secure admin access
Secure routed connection between clients allows for file transfers

The Digi TransPort implementation of OpenVPN can be configured as an OpenVPN server (shown above) or as an OpenVPN client, connecting to an OpenVPN server.

On TransPort firmware, OpenVPN has been implemented as an interface. That means that when an OpenVPN tunnel connects, an interface is added to the routing table. Static routes may be configured to point to an OpenVPN instance, and additionally, OpenVPN may learn routes from the tunnel peer and add these routes to the routing table for the duration of the OpenVPN tunnel. As each tunnel appears just like an interface, support for features like the firewall, NAT, IGMP etc are the same as for other interfaces like PPP and ETH.

OpenVPN n

Configuration - Network > Virtual Private Networking (VPN) > OpenVPN > OpenVPN n

Description
The text string is a friendly name to help identify this OpenVPN instance.

IP address a.b.c.d
This must be specified correctly. OpenVPN interfaces use a 30 bit mask, the first address is the network address, the 2nd is the server address, the 3rd is the client address, the 4th is the broadcast address. This address must be configured as the 2nd IP address in the block of 4. For example 192.168.0.1 if configured as a server, or 192.168.0.2 if configured as a client.

Destination host a.b.c.d
Only required when configured as an OpenVPN client. This is the IP address of the OpenVPN server.

Link socket interface x,y
If configured, OpenVPN sockets will only be allowed to/from this interface and the routing table will be ignored. When set to Auto, the OpenVPN sockets will use the routing table to identify the best interface to use.

Get link socket source address from this interface x,y
The values in these two text boxes define the interface (Auto,PPP,ETH) and the instance number of the interface to use as a source address for IP sockets when not using the interface that the socket was created on.
Even when this parameter is not configured, the IP address from the interface on which the socket was created will be used. The source address specified in this parameter will only be used if it will cause the traffic to match an Eroute and therefore be sent using IPsec or GRE.

MTU
This parameter is used to set the Maximum Transmit Unit for the OpenVPN instance, in bytes. The default setting is 1400.

Metric
This parameter specifies the connected metric, changing this value will alter the metric of dynamic routes created automatically for this interface.

NAT mode
This parameter is used to select whether IP Network Address Translation (NAT) or Network Address and Port Translation (NAPT) are used at the Ethernet interface. When the parameter is set to disabled, no NAT will take place.

IP analysis
When enabled, the un-encapsulated IP traffic will be captured into the analyser trace.

Firewall
The Firewall parameter is used to turn Firewall script processing “On” or “Off” for this interface.

IGMP
This IGMP parameter is used to enable or disable the transmission and reception of IGMP packets on this interface. IGMP is used to advertise members of multicast groups. If IGMP is enabled, and a member of a multicast group is discovered on this interface, multicast packets for this group received on other interfaces will be sent out this interface.

Include in RIP advertisements
When checked, this checkbox will cause the router to include this static route to be included in RIP advertisements.

Automatically connect interface
If enabled, this OpenVPN instance will be considered as an always on interface.

Server mode (listener)
This parameter configures the OpenVPN instance to listen for inbound OpenVPN sockets.

Link socket port
The default port used by OpenVPN is 1194. If a different or non-standard port number is used, specify it here.

Link socket protocol
OpenVPN can use TCP or UDP as the transport protocol. Select the required protocol here.

Use plain string for TLS Auth Key

Select this when TLS Authoorization key is a string.

TLS auth password / Confirm TLS auth password

This allows the OpenVPN instance to use an extra level of security by having a TLS password configured.

Use file for TLS Auth Key

Select this when TLS Authoorization key is a file.

TLS password filename
Select the filename of the OpenVPN TLS authentication key from this drop-down list.

TLS Auth Key direction
Select the authentication key direction for usage of different tx and rx authentication key files. This is enabled when TLS Authoorization key is a file.

User Name
This is the user name sent to remote peer.

Password
This is the password sent to remote peer

Require remote peer to supply Username and Password
This Boolean field is turned ON if the remote is required to send username/password. If it is ON and the remote peer fails to send username/password, the negotiation will fail. If it is turned OFF, the username/password from the remote peer is ignored.

Push IP address #1/#2/#3
When configured as an OpenVPN server, these parameters can be used to push subnets to the client that need to be routed via the OpenVPN server. Used in conjunction with the Push Mask parameter below.

Push mask #1/#2/#3
Used with the Push IP address parameter above to define subnets that should be routed via the OpenVPN server.

Push DNS server address #1/#2
When configured as an OpenVPN server, these parameters can be used to push DNS server settings to the OpenVPN client.

Pull interface IP address
When configured as an OpenVPN client, this option must be enabled for the router to obtain and use the local IP address supplied from the OpenVPN server.

Pull routes
When configured as an OpenVPN client, this option must be enabled for the router to use routes sent from the OpenVPN server.

Pull DNS server addresses
When configured as an OpenVPN client, this option must be enabled for the router to use DNS servers sent from the OpenVPN server.

Packet replay ID window
When set to a non-zero value, this enables sequence number replay detection. It indicates the number of packet IDs lower than the current highest ID to allow out of sequence.

Packet replay time window (seconds)
Set to a non-zero value to enable time tracking of incoming packets.

OpenVPN TX ping interval (seconds)
Interval between OpenVPN ping transmissions. These are required to detect the operational state of the VPN connection.

OpenVPN RX ping timeout (seconds)
The number of seconds, after which no OpenVPN ping has been received, the VPN will be marked as down.

Include IV
Enabling this option on includes an IV at the head of an encrypted packet. If one peer prepends this IV and the other isn't expecting it, packet decryption will fail.

Key negotiation timeout (seconds)
Maximum time in seconds to allow for a data channel key negotiation.

Key renegotiation interval (seconds)
Interval between key re-negotiations.

Key renegotiation bytes
If non-zero, a key renegotiation will take place after this many bytes have travelled through the data channel (in either direction).

Key renegotiation packets
If non-zero, a key renegotiation will take place after this many packets have travelled through the data channel.

Inactivity timeout (seconds)
The tunnel is disconnected after the tunnel becomes inactive (no IP traffic) for this many seconds. Note that the timer is only restarted with RX traffic, not TX traffic.

Data channel cipher
Sets the cipher used for data channel encryption/decryption. Select from the dropdown list.

Data channel digest
Sets the digest algorithm used for data channel authentication. Select from the dropdown list.

Debug
Enables output of OVPN related debug.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ovpn	n	descr	Up to 30 characters	Description
ovpn	n	IPaddr	Valid IP address a.b.c.d	IP address a.b.c.d
ovpn	n	dest	Valid IP address a.b.c.d	Destination host a.b.c.d
ovpn	n	ll_ent	<blank>, PPP, ETH	Link socket interface x,y x= interface type
ovpn	n	ll_add	0 - 2147483647	Link socket interface x,y y= interface number
ovpn	n	ip_ent	<blank>, PPP, ETH	Get link socket source address from this interface x,y x= interface type
ovpn	n	ip_add	0 - 2147483647	Get link socket source address from this interface x,y y= interface number

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ovpn	n	mtu	0 - 2147483647	MTU
ovpn	n	metric	0 - 2147483647	Metric
ovpn	n	do_nat	0,1,2 0 = Off 1 = Address only 2= Address and port	NAT mode
ovpn	n	ipanon	OFF,ON	IP analysis
ovpn	n	firewall	OFF,ON	Firewall
ovpn	n	igmp	OFF,ON	IGMP
ovpn	n	inrip	OFF,ON	Include in RIP advertisements
ovpn	n	autoup	OFF,ON	Automatically connect interface
ovpn	n	server	OFF,ON	Server mode (listener)
ovpn	n	port	0 - 65535	Link socket port
ovpn	n	proto	TCP,UDP	Link socket protocol
ovpn	n	tls_auth_key	Up to 30 characters	TLS auth password
ovpn	n	etls_auth_key		enciphered version TLS auth password
ovpn	n	tlskeyfil	key file name in 8.3 format	TLS password filename
ovpn	n	tlskeydir	0,1,2 0: Bidirectional 1: Normal 2: Inverse	TLS Auth Key direction
ovpn	n	username	Up to 20 characters	User Name
ovpn	n	password	Up to 20 characters	Password
ovpn	n	req_unpw	OFF, ON	Require remote peer to supply Username and Password
ovpn	n	puship	Valid subnet a.b.c.d	Push IP address #1 a.b.c.d
ovpn	n	pushmask	Valid netmask a.b.c.d	Push mask #1 a.b.c.d
ovpn	n	puship2	Valid subnet a.b.c.d	Push IP address #2 a.b.c.d
ovpn	n	pushmask2	Valid netmask a.b.c.d	Push mask #2 a.b.c.d

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ovpn	n	puship3	Valid subnet a.b.c.d	Push IP address #3 a.b.c.d
ovpn	n	pushmask3	Valid netmask a.b.c.d	Push mask #3 a.b.c.d
ovpn	n	pushdns	Valid IP address a.b.c.d	Push DNS server address #1 a.b.c.d
ovpn	n	pushdns2	Valid IP address a.b.c.d	Push DNS server address #2 a.b.c.d
ovpn	n	pullip	OFF,ON	Pull interface IP address
ovpn	n	pullroute	OFF,ON	Pull routes
ovpn	n	pulldns	OFF,ON	Pull DNS server addresses
ovpn	n	sreplay	0 - 2147483647	Packet replay ID window
ovpn	n	treplay	0 - 2147483647	Packet replay time window (seconds)
ovpn	n	pingint	0 - 2147483647	OpenVPN TX ping interval (seconds)
ovpn	n	pingto	0 - 2147483647	OpenVPN RX ping timeout (seconds)
ovpn	n	inciv	OFF,ON	Include IV
ovpn	n	neg_timeout	0 - 2147483647	Key negotiation timeout (seconds)
ovpn	n	reneg_int	0 - 2147483647	Key renegotiation interval (seconds)
ovpn	n	reneg_bytes	0 - 2147483647	Key renegotiation bytes
ovpn	n	reneg_packets	0 - 2147483647	Key renegotiation packets
ovpn	n	inact_timeout	0 - 2147483647	Inactivity timeout (seconds)
ovpn	n	cipher	See cipher list below	Data channel cipher
ovpn	n	digest	See digest list below	Data channel digest
ovpn	n	debug	OFF,ON	Debug

Supported Cipher and Digest values for OpenVPN

Cipher values	Digest values
DES-EDE-CBC	md2WithRSAEncryption
AES128	ssl2-md5
DES	MD5
DES-CBC	sha1WithRSAEncryption

Cipher values	Digest values
AES-128-CBC	ssl3-sha1
AES192	ssl3-md5
AES-192-CBC	SHA1
DES-EDE3-CBC	MD2
AES-256-CBC	RSA-MD2
AES-256	md5WithRSAEncryption
DES3	RSA-SHA1
Blowfish	RSA-SHA1-2
	RSA-MD5
	SHA256

SSL

Configuration – Network > SSL

The secure socket layer (SSL) that provides a secure transport mechanism is supported by Digi's TransPort routers. The configuration of the client-side and server (***Configuration – Network > SSL*** webpage) are described in the following pages.

SSL Clients

Configuration – Network > SSL> SSL Clients

Some sites require client side authentication when connecting to them. The router's SSL client handles the authentication for SSL connections using certificates signed by a Certificate Authority (CA). For more information regarding certificates and certificate requests, refer to the certificates page ***Administration – X.509 Certificate Management > Certificate Authorities (CAs)***.

Configuring the SSL clients is handled by a table having the columns and parameters listed below:

SSL Client
This column is simply a list of the SSL client numbers supported by the router.

Client Certificate Filename
The name of the required certificate file is selected from those available on the router's filing system from this drop-down list.

Client Private Key Filename
The name of the file that contains the private key that matches the public key stored in the above parameter, is selected from this drop-down list.

Cipher List
The cipher list in this text box is a list of one or more cipher strings separated by colons. Commas or spaces are also accepted as separators but colons are normally used. The actual cipher string can take several different forms. It can consist of a single cipher suite such as RC4-SHA. It can represent a list of cipher suites containing a certain algorithm or cipher suites of a certain type. For example, SHA1 represents all cipher suites using the SHA1

digest algorithm and SSLv3 represents all SSL v3 algorithms. Lists of cipher suites can be combined in a single cipher string using the "+" character. This forms the logical **AND** operation. For example, SHA1+DES represents all cipher suites containing SHA1 and DES algorithms. If left empty, the cipher list is not used.
For more information see: http://www.openssl.org/docs/apps/ciphers.html

Apply to Destination IP Address
The value in this text box allows the configuration of multiple SSL destinations, each having a different certificate/key pair. When set, this parameter will lock the SSL client settings to a specific IP address. If this parameter is left blank, the configured SSL client settings will be used for any connection that requires SSL.

As is usual with the tables on the configuration web pages, the relevant and appropriate parameters are selected and the **Add** button on the right-hand side is clicked to add the entry into the table. Once an entry has been added, it may be removed by clicking the **Delete** button that will appear in the right-hand column.

Verify Server Certificate

This parameter allows enabling server certificate verification. When enabled, if the server certificate chain is unable to be verified (need CA certificate installed onto the unit), the SSL negotiation will fail.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
sslcli	0 - 5	certfile	Up to 12 characters (DOS 8.3 format)	Client Certificate Filename
sslcli	0 - 5	keyfile	Up to 12 characters (DOS 8.3 format)	Client Private Key Filename
sslcli	0 - 5	cipherlist	Colon-separated list of ciphers	Cipher List
sslcli	0 - 5	IPaddr		Apply to Destination IP Address
sslcli	0 - 5	verify	OFF,ON	Verify Server Certificate

SSL Server

Configuration – Network > SSL > SSL Server

This page describes the parameters needed to configure the SSL server.

Server Certificate Filename
The file containing the server certificate is selected from this drop-down list.

Client Private Key Filename
The file containing the private key that matches the above certificate is selected from this drop-down list.

SSL Version
The version of the SSL protocol to use, is selected from this drop-down list. Selecting "Any" allows the use of any version. The available options are:

- Any
- TLSv1 only

- SSLv3 only
- SSLv2 only.

Cipher List
The list of ciphers is the same as described above for the client-side configuration table.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
sslsvr	0	certfile	Up to 12 characters (DOS 8.3 format)	Server Certificate Filename
sslsvr	0	keyfile	Up to 12 characters (DOS 8.3 format)	Server Private Key Filename
sslsvr	0	ver	Blank, TLS1, SSL3, SSL2	SSL Version
sslsvr	0	cipherlist	Colon-separated list	Cipher List
sslsvr	0	debug	OFF,ON	n/a

SSH Server

Configuration – Network > SSH Server

The secure shell (SSH) server allows remote peers to access the router over a secure TCP connection using a suitable SSH client. The SSH server provides a Telnet-like interface and secure file transfer capability.

SSH uses a number of keys during a session. The host keys are used for authentication purposes. Keys unique to each SSH session are also generated and are used for encryption/authentication purposes.

The router supports SSH v1.5 and SSH v2. The host key file format differs for each version but there would normally only be one host key for each version. For this reason the router allows the user to configure two host key files. These keys may be changed from time to time, specifically if it suspected that the key has become compromised. Because the host keys need to be secure, it is highly recommended to store the files on the router's FLASH filing system using filenames prefixed with "priv" which makes it impossible to read the files using any of the normal methods (e.g. FTP). It is possible (using the **genkey** command) to create host keys in either format for use with SSH. Using this utility it is not necessary to have the host key files present on any other storage device (thus providing an additional level of security). Refer to the section of this manual that covers certificates on how to generate a private key file.

Unlike the Telnet server it is possible to configure the number of SSH server sockets that listen for new SSH connections.

Multiple SSH server instances can be configured, each instance can be configured to listen on a separate port number and can use different keys and encryption methods.

It is possible to configure which authentication methods can be used in an SSH session and the preferred selection order. The router currently supports MD5, SHA1, MD5-96 and SHA1-96. If required, a public/private key pair can be used for authentication.

The router currently supports 3DES, 3DES-CBC and AES cipher methods.

DEFLATE compression is also supported. If this is enabled and negotiated, SSH packets are first compressed before being encrypted and delivered to the remote unit via the TCP socket.

Note:
The SSH server supports the SCP file copy protocol but does NOT support filename wildcards.

Enable SSH Servers
When checked, this checkbox enables the SSH servers on the router.

SSH Server n

Configuration – Network > SSH Server> SSH Server n

The router supports eight individual SSH servers that are configured independently using the options described below.

Enable SSH Server
When checked, this checkbox enables the SSH server.

Use TCP port p
The value in this text box is the TCP port number (default 22) that the SSH server will use to listen for incoming connections. (Port 22 is the standard SSH port).

Allow up to n connections
The value in this text box specifies the number of sockets listening for new SSH connections (default 1).

Host Key 1 Filename
The value in this text box is the filename of either an SSH V1 or V2 host key. It is highly recommended that the filename be prefixed with "priv" to ensure that the key cannot be easily accessed and compromised. This key may be generated using the facilities described in the Certificates section of this manual.

Host Key 2 Filename
The value in this text box is the filename of either an SSH V1 or V2 key as above.

Note:
The maximum length for these filenames is 12 characters and they must use the DOS 8.3 file naming convention.

Maximum login time s seconds
The value in this text box specifies the maximum length of time (in seconds) that a user is allowed to successfully complete the login procedure once the SSH socket has been opened. The socket is closed if the user has not completed a successful login within this period.

Maximum login attempts n
The value in this text box specifies the maximum number of login attempts allowed in any one session before the SSH socket will be closed.

Use Deflate compression No/Yes, level n
The radio buttons select whether or not DEFLATE compression will be used. If compression is selected, the compression level is chosen from the drop-down list.

Enable Port Forwarding

When checked, this checkbox enables the router to accept traffic on ports other than 23. This functionality is for use with SSH client applications (such as PuTTY) that has port forwarding capability. For example, one the SSH connection is active, traffic for the HTTP port 80 can be sent to the router securely.

Command Session IP Address a.b.c.d Port p
The values in these two text boxes are used to specify the host IP address and port number that the router will use to handle incoming requests for a command session from SSH clients. This is instead of the router's normal command interpreter. For example, if the values are IP address 127.0.0.1, port 4000, the SSH client will make a direct connection to ASY 0 and the device attached to ASY 0 will receive and process the commands from the SSH client.

Enable support for SSH v1.5
When checked, this checkbox allows the server to negotiate SSH V1.5. The router must also have a SSH V1 key present and the filename entered into the SSG configuration.

Server key size
This option applies to V1 SSH. During initialisation of an SSH session, the server sends its host key and a server key (which should be of a different size to the host key). The router generates this key automatically but the length of the server key is determined by this parameter. If when this value is set it is too similar to the length of the host key, the router will automatically adjust the selected value so that the key sizes are significantly different.

Enable support for SSH v2.0
When checked, this checkbox allows the server to negotiate SSH V2. The router must also have a SSH V2 key present and the filename entered into the SSG configuration.

Actively start key exchange
This option applies to V2 SSH. Some SSH clients wait for the server to initiate the key exchange process when a new SSH session is started unless they have data to send to the server, in which case they will initiate the key exchange themselves. When checked, this checkbox will cause the router to automatically initiate a key exchange without waiting for the client.

Rekey Never / After n units of data have been transferred
With SSH V2 it is possible to negotiate new encryption keys after the current ones have been used to encrypt a specified amount of data. The radio buttons select whether this feature should be used. If this feature is to be used the amount of data is entered into the text box and the applicable units (Kbytes, Mbytes, Gbytes) selected from the drop-down list.

Encryption Preferences
The following four configuration options allocate preferences to the encryption method that should be used to encrypt data on the link. A lower value indicates greater preference apart from zero which disables the option.

3DES
The value in this text box is the preference level for the Triple-DES algorithm.

AES (128 bits)
The value in this text box is the preference level for the 128-bit AES algorithm.

AES (192 bits)
The value in this text box is the preference level for the AES algorithm using 192 bits.

AES (256 bits)
The value in this text box is the preference level for the AES algorithm using 256 bits.

Authentication Preferences

The following four configuration options allocate preferences to the authentication methods that should be used. As above, a value of zero disables the particular authentication method and lower values indicated greater preference than higher values. So, for example if MAC SHA1-96 was the preferred method for authentication, this option would be given the value 1 and the other options given a value of 2 or greater. If all these parameters are set to the same value, the router automatically uses them in the following order: SHA1, SHA1-96, MD5, MD5-96.

MAC MD5
The value in this text box is the preference level for MAC MD5.

MAC MD5-96
The value in this text box is the preference level for MAC MD5-96.

MAC SHA1
The value in this text box is the preference level for MAC SHA1.

MAC SHA1-96
The value in this text box is the preference level for MAC SHA1-96.

Enable Debug
The router supports logging and output of debugging information for situations where there are problems establishing a SSH connection. When checked, this checkbox causes the router to trace and output information that should be helpful in diagnosing and resolving the problem.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ssh	0 – 7	port	0 - 65535	Use TCP port p
ssh	0 - 7	nb_listen	0 - 2147483647	Allow up to n connections
ssh	0 - 7	hostkey1	Up to 12 characters (8.3 format)	Host Key 1 Filename
ssh	0 - 7	hostkey2	Up to 12 characters (8.3 format)	Host Key 2 Filename
ssh	0 - 7	loginsecs	0 - 2147483647	Maximum login time s seconds
ssh	0 - 7	logintries	0 - 2147483647	Maximum login attempts n
ssh	0 - 7	comp	0 = disabled	Use Deflate compression , level
ssh	0 - 7	fwd	0 - 2147483647	Enable port forwarding
ssh	0 - 7	cmdhost	Valid IP address a.b.c.d	Command session IP address a.b.c.d
ssh	0 - 7	cmdport	0 - 2147483647	Command session port p
ssh	0 - 7	svrkeybits	0 - 2147483647	Server key size
ssh	0 - 7	initkex	OFF,ON	Actively start key exchange
ssh	0 - 7	rekeybytes	0 - 2147483647 0 = Do not rekey	Rekey After n units of data have been transferred
ssh	0 - 7	enc3descbc	0 - 2147483647	3DES

Entity	Instance	Parameter	Values	Equivalent Web Parameter
			0 = Disabled	
ssh	0 - 7	encaes128cbc	0 - 2147483647	AES (128 bits)
ssh	0 - 7	encaes192cbc	0 - 2147483647	AES (192 bits)
ssh	0 - 7	encaes256cbc	0 - 2147483647	AES (256 bits)
ssh	0 - 7	macmd5	0 - 2147483647	MAC MD5
ssh	0 - 7	macmd596	0 - 2147483647	MAC MD5-96
ssh	0 - 7	macsha1	0 - 2147483647	MAC SHA1
ssh	0 - 7	macsha196	0 - 2147483647	MAC SHA1-96
ssh	0 - 7	debug	0,1 0 = Off 1 = On	Enable Debug

Configuring SSH

In order to fully configure SSH, a version1 SSH key and a version 2 SSH key need to be generated and the router configured to use them. This procedure will be described below.

Note:
SSH version 2 is more secure than version 1 and so is the recommended version to use. However, some SSH clients may only support version 1 keys and so the router supports both version 1 and version 2 SSH.

Configuration using the web interface

Navigate to ***Administration – X.509 Certificate Management > Key Generation*** and select the size of the key file from the drop-down list. The larger the key file, the more secure it will be.

Enter the name for the key file in the **Key filename** box or select from those already present using the drop-down selector. The filename should have a prefix of “priv” and a file extension of “.pem”, e.g. “privssh1.pem”. (Please note that the 8.3 file name convention applies as mentioned previously).

Check the checkbox marked **Save in SSHv1 format** in order to generate a version 1 SSH key. Click the **Generate Key** button to generate the private key file. The key file will be stored in the router’s FLASH filing system.

Repeat steps 1 to 3 in order to generate the second key. This time, however, make sure that the **Save in SSHv1 format** checkbox is unchecked. This key file should be given a different name to the version 1 file previously generated.

On the ***Configuration – Network > SSH Server > SSH Server n*** page, enter the filename generated in step 3 into the **Host Key 1 Filename** text box and the filename generated in step 4 into the **Host Key 2 Filename** text box.

Apply the configuration changes using the Apply button at the bottom of the page and when the “Configuration successfully applied” message appears, click on the highlighted link to save the configuration.

Configuration using the command line interface

Generate the SSH V1 private key using the **genkey** command as follows:

genkey <keybits> <filename> -ssh1 where *<keybits>* is one of the following values; 384, 512, 768, 1024, 1536 or 2048 and *<filename>* is the name for the file, e.g. "privssh1.pem" as described for the web version of this procedure.

Generate the SSH V2 private key using the **genkey** command as per step 1 but this time omit the *–ssh1* switch. For example:

genkey 1024 privssh2.pem.

Set the first private key as the SSH Host key 1 using the following command:

ssh 0 hostkey1 privssh1.pem

Set the second private key as SSH Host Key 2 using the following command:

ssh 0 hostkey2 privssh2.pem

Save the configuration:

config 0 save

SSH Authentication with a public/private keypair

Once SSH access has been configured and confirmed to be working, RSA key pair authentication can be added and used to replace password authentication.

This process will involve the use of PuTTYgen to create public and private keys. Please see the Technical Notes section on the Digi website for full details on how to perform this procedure.

FTP Relay

Configuration – Network > FTP Relay

The FTP Relay agents allow any files to be transferred onto the router by a specified user using the File Transfer Protocol to be temporarily stored in memory and then relayed to a specific FTP host. This is useful when the router is being used to collect data files from a locally attached device such as a webcam which must then be to a host system over a slower data connection such as W-WAN. In effect, the router acts as a temporary data buffer for the files.

The FTP Relay Agent may also be configured to email (as an attachment) any file that it was unable to transfer to the FTP server. To facilitate this, set the Email Template, To, From and Subject parameters as appropriate and also configure the SMTP client (***Configuration – Alarms > SMTP Account***).

FTP Relay n

Configuration – Network > FTP Relay> FTP Relay n

There are two FTP Relay Agents available, with a separate web page for each. For command line configuration, the instance number can be 0 or 1.

Relay files for user locuser to FTP Server ftphost

The value in the left-hand text box is the name of the local user and should be one of the usernames assigned in the ***Configuration – Security > Users*** web page. This name is then used as the FTP login username when the local device needs to relay a file. The value in the right-hand text box is the name of the FTP host to which the files from the locally attached device are to be relayed.

Server Username
The value in this text box is the username required to log in to the specified FTP host.

Server Password
The value in this text box specifies the password to be used to log in to the host.

Confirm Server Password
The password should be retyped into this text box in order to confirm that it has been entered correctly, given that it is not echoed in clear text.

Remote directory
The value in this text box is the full name of the directory on the FTP host to which the file is to be saved.

Rename file
When checked, this checkbox causes the router to store the uploaded files internally with a filename in the form "relnnnn" where nnnn is a number that is incremented for each new file received. When the file is relayed to the FTP host the original filename is used. When unchecked, the file is stored internally using its original filename. This parameter should be set if it a file having a filename longer than 12 characters is to be uploaded. This is due to the internal file system having the 8.3 filename format (i.e. autoexec.bat).

Transfer Mode ASCII / Binary
These two radio buttons select between the two possible file transfer modes, binary data or ASCII data.

Transfer Command STORE / APPEND
These two radio buttons select between the two possible storage methods, either append to or replace existing file.

Attempt to connect to the FTP Server n times
The value in this text box specifies the number of connection attempts that the router should make if the first attempt is not successful.

Wait s seconds between attempts
The value in this text box specifies the interval (in seconds) that the router should wait in between successive connections attempts.

Remain connected for s seconds after a file has been transferred
The value in this text box specifies how long (in seconds) that the router will maintain the connection to the FTP host after transferring a file.

If unable to relay file Delete File / Retain file
These two radio buttons select the behaviour with respect to storing the file if the router fails to connect to the FTP host (after retrying for the specified number of attempts). Select Delete File if the file should not be stored permanently. If the file is retained, manual intervention will be required to recover it at a later stage.

Note:
If the file is not retained, it will be lost if the power is removed from the router.

Email the file before storing or deleting it

The configuration options following this checkbox are normally disabled (they should appear "greyed out" in the browser). When this checkbox is checked, the parameters are enabled and data can be entered into the text boxes.

Use Email Template File
The value in this text box contains the name of the template file that will be used to form the basis of any email messages generated by the FTP Relay Agent. This would normally be the standard "**EVENT.EML**" template provided with the router but alternative templates may be created if necessary (refer to Email templates elsewhere in this manual).

To
The value in this text box is used to specify the email address of the recipient of email messages generated by the FTP Relay Agent.

From
The value in this text box is used to specify the email address of the router. In order for this to work, an email account must be in place with the Internet Service Provider.

Subject
This text box should contain a brief description of the content of the email.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
frelay	n	locuser	Up to 15 characters	Relay files for user locuser
frelay	n	ftphost	Up to 64 characters	to FTP Server ftphost
frelay	n	ftpuser	Up to 20 characters	Server Username
frelay	n	ftppwd	Up to 20 characters	Server Password
frelay	n	ftpdir	Up to 40 characters	Remote directory
frelay	n	norename	OFF,ON	Rename file
frelay	n	ascii	OFF,ON	Transfer Mode
frelay	n	appe	OFF,ON	Transfer Command
frelay	n	retries	0 - 2147483647	Attempt to connect to the FTP Server n times
frelay	n	retryint	0 - 2147483647	Wait s seconds between attempts
frelay	n	timeout	0 - 2147483647	Remain connected
frelay	n	savemode	OFF,ON	Delete/Retain file
frelay	n	smtp_temp	Up to 40 characters	Use Email Template File
frelay	n	smtp_to	Up to 100 characters	To
frelay	n	smtp_from	Up to 40	From

Entity	Instance	Parameter	Values	Equivalent Web Parameter
			characters	
frelay	n	smtp_subject	Up to 40 characters	Subject

Advanced

Configuration – Network > FTP Relay> Advanced

Tx Buffer Size n bytes
The value in this text box specifies the size of the Tx socket buffer.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ftpcli	n	txbuf	0 - 2147483647	Tx Buffer Size

IP Passthrough

Configuration – Network > IP Passthrough

IP passthrough is a useful feature if a host computer or server on the local area network needs to have access to it from the Internet with a public IP address. With IP passthrough configured, all IP traffic, not just TCP/UDP is forwarded back to the host computer. This feature can be useful for applications that do not function reliably through network address translation.

In this configuration the local PC will share the public IP addressing information with the WAN side of the router.

Enable IP Pass-through
When checked, this checkbox enables IP passthrough mode.

Ethernet interface
The value in this text box specifies the Ethernet interface that the local PC is connected to.

PPP interface
The value in this text box specifies the PPP interface that will share its WAN address with the local PC.

Mode
This drop-down list selects the the mode of operation for the passthrough functionality. The available options are **Normal/24 bit mask** and **Fixed IP Address/32 bit mask**. The default is **Normal/24 bit mask**. When **Fixed IP/32 bit mask** mode of operation is selected, the DHCP server will provide a 32-bit subnet mask to the client and sets the address/subnet mask for the Ethernet interface to 192.168.1.1/32.

Pinhole Configuration
The following parameters are checkboxes that allow specific protocols to be excluded from the IP passthrough feature. An excluded protocol will terminate at the router instead of being forwarded to the local PC.

HTTP
When checked, this checkbox excludes HTTP from passthrough.

HTTPS
When checked, this checkbox excludes HTTPS from passthrough.

Telnet
When checked, this checkbox excludes Telnet from passthrough.

Telnet over SSL
When checked, this checkbox excludes SSL from passthrough.

SSH / SFTP
When checked, this checkbox excludes SSH/SFTP from passthrough.

SNMP
When checked, this checkbox excludes SNMP from passthrough.

Device Cloud
When checked, this checkbox excludes the device cloud protocol from passthrough.

Note:
This option only appears on models that support the device cloud remote management functionality.

GRE
When checked, this checkbox excludes GRE from passthrough.

Ping
When checked, this checkbox excludes the ICMP echo request from passthrough.

Other Ports
The list of TCP and UDP port numbers in this text box will be added to the list that will not be forwarded to the local PC (comma-separated).

Other Protocols
The list of protocol numbers in this text box will be added to the list that will not be forwarded on to the local PC (comma-separated).

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
passthru	0	enabled	OFF,ON	Enable IP Pass-through
passthru	0	ethadd	0 - 2147483647	Ethernet interface
passthru	0	pppadd	0 - 2147483647	PPP interface
passthru	0	mode	0,1 0 = Normal 1 = 32-bit mask	Mode
passthru	0	http	OFF,ON	HTTP
passthru	0	https	OFF,ON	HTTPS
passthru	0	telnet	OFF,ON	Telnet
passthru	0	telnets	OFF,ON	Telnet over SSL
passthru	0	ssh	OFF,ON	SSH/SFTP
passthru	0	snmp	OFF,ON	SNMP
passthru	0	cloud	OFF,ON	Device Cloud
passthru	0	gre	OFF,ON	GRE
passthru	0	ping	OFF,ON	Ping

Entity	Instance	Parameter	Values	Equivalent Web Parameter
passthru	0	ports	Comma-separated list of ports	Other Ports
passthru	0	protos	Comma-separated list of protocols	Other Protocols

UDP Echo

Configuration – Network > UDP Echo

When enabled, the UDP echo client generates UDP packets that contain the router's serial number and ID and transmits them to the IP address specified by the configuration. When the remote router receives a UDP packet on a local port and UDP echo server is configured, it will echo the packet back to the sender. There may be more than one UDP echo instance available on the unit. Instance 0 is used when specifying the local port to listen on.

UDP Echo n

Configuration – Network > UDP Echo > UDP Echo n

There may be instances of the UDP echo task supported by the router (model-dependent). Each has its own configuration web page, described below. For the command line configuration, valid instance numbers start at 0 as normal.

Enable UDP Echo
This checkbox is unchecked by default – when checked, it reveals the configuration parameters associated with send UDP echo packets.

Send a UDP packet to IP address a.b.c.d port n every s seconds
The values in these three text boxes define the destination IP address for the UDP packets, the port number to which they should be sent and the sending interval. If the destination IP address is left blank, the router will not attempt to send any packets.

Use local port n
The value in this text box specifies which local port the router should listen on for UDP packets. If any UDP packets are sent to this port, the router will send a copy back to the IP address and port they were sent from.

Route via Routing table / Interface x,y
These two radio buttons select whether the router should use its routing table to determine how to send the UDP packets or whether it should use the specified interface. If the specific interface is selected, the interface is selected from the drop-down list. The options available are PPP and Ethernet. The interface instance is specified in the adjacent text box.

Only send packet when the interface is "In Service"
When checked, and the router is using the specified interface, this checkbox will prevent the router from sending UDP packets if the interface is out of service.

Do not send any data with the UDP packet
When checked, this check box causes the router to send only a single null data byte. This is useful to minimise packet size in circumstances where the interface has high data charges (e.g. W-WAN). When unchecked, the router will send packets that contain the router's serial number and ID as text.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter

Entity	Instance	Parameter	Values	Equivalent Web Parameter
udpecho	n	dstip	Valid hostname	Send a UDP packet to IP address a.b.c.d port n every s seconds
udpecho	n	dstport	0 - 65535	Send a UDP packet to IP address a.b.c.d port n every s seconds
udpecho	n	interval	0 - 2147483647	Send a UDP packet to IP address a.b.c.d port n every s seconds
udpecho	n	locport	0 - 65535	Use local port n
udpecho	n	userouting	OFF,ON	Route via Routing table
udpecho	n	ifent	PPP,ETH	Interface x,y
udpecho	n	ifadd	Valid interface instance 0 - 4294967296	Interface x,y
udpecho	n	onlyis	OFF,ON	Only send packet when the interface is “In Service”
udpecho	n	nodata	OFF,ON	Do not send any data with the UDP packet

QoS

Configuration – Network > QoS

The Quality of Service (QoS) functionality provides the means of prioritising different types of IP traffic. It is generally used to ensure that low priority applications do not “hog” the available bandwidth to the detriment of those having a higher priority. For example, this might mean that EPOS transactions carried out over XOT will be prioritised over HTTP-type traffic used for Internet access. Without some form of QoS, all IP packets are treated as being equal, i.e. there is no discrimination between applications.

The IP packet Type of Service (TOS) field is used to indicate how a packet should be prioritised. Using the top 6 bits of the TOS field, a router that supports QoS will assign a Differentiated Services Code Point (DSCP) code to the packet. This may take place within the router when it receives the packet or another router closer to the packet source may have already assigned it. Based on the DSCP code, the router will assign the packet to a priority queue. There are currently four such queues for each PPP instance within the router and each queue can be configured to behave a particular way so that packets in that queue are prioritised for routing according to predefined rules.

There are two principal ways in which prioritisation may be effected:

A priority queue can be configured to allow packets to be routed at a specific data rate (providing that queues of a higher priority are not already using the available bandwidth)

Weighted Random Early Dropping (WRED) of packets may be used as queues become busy, in an attempt to get the TCP socket generating the packets to “back off” its transmit timers, thus preventing the queue overflow (which would result in all subsequent packets being dropped).

QoS is a complex subject and can have a significant impact on the performance of the router. For detailed background information on QoS, refer to RFC2472 (Definition of the Differentiated Services Field).

In Digi TransPort routers, the classification of incoming IP packets for the purposes of QoS takes place within the firewall. The firewall allows the system administrator to assign a DSCP code to a packet with any combination of source/destination IP address/port and protocol. Details of how this is done are given in the section on firewall scripts.

When the routing code within the unit receives an incoming packet, it directs it to the interface applicable to that packet at that time (this is the case whether or not QoS is being applied). Just before the packet is sent to the interface, the QoS code intercepts the packet and assigns it to one of the available priority queues (currently 10 per PPP instance) based on its DSCP value.

Each priority queue has a profile assigned to it. This profile specifies parameters such as the minimum transmit rate to attempt, maximum queue length and WRED parameters.

The packet is then processed by the queue management code and either dropped or placed in the queue for later transmission.

There are a couple of configuration web pages associated with QoS functionality:

- DSCP Mappings
- Queue Profiles

The ***Configuration – Network > QoS > DSCP Mappings*** page which contains parameters to configure DSCP operation and ***Configuration – Network > Queue Profiles*** page which contains parameters to manage the queue "profiles".

Each ***Configuration – Interfaces > Ethernet*** and ***Configuration – Interfaces > PPP*** instance page contains a QoS sub-page which control how QoS behaves on that particular interface.

When configuring QoS, be aware that the router supports ten queues, numbered from 0 to 9 and that DSCP codes range from 0 to 64.

DSCP Mappings

Configuration – Network > QoS > DSCP Mappings

Each DSCP value must be mapped to a queue. These mappings are set up using this page.

Default
This drop-down list selects the default queue. When this is changed, any DSCP codes that are set to use the default will have their queue number changed.

DSCP
This column is simply a list of valid DSCP codes with an associated drop-down list box to the right.

Queue
Each of the DSCP codes in the left-hand column has a queue associated with it. To change the value from what is shown, select the desired value from the drop-down list.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
dscp	n	q	0 – 63	Queue

Entity	Instance	Parameter	Values	Equivalent Web Parameter
			Default 4	

Example command line commands.

To display a DSCP mapping from the command line, type the following:

dscp <code> ?

Where <*code*> is a valid DSCP code from 0 to 63, or 64 (but see note below).

To change the value of a parameter, use the following command:

dscp <code> q <value>

Where <*code*> is a valid DSCP code and <*value*> is from 0 to 9.

To set the default mapping value, enter the command:

dscp 64 q <value>

Where <*value*> is the default queue number required and has a value from 0 to 9.

Note:
DSCP code 64 is not actually a valid code but is used to set up the default priority.

Queue Profiles

Configuration – Network > QoS> Queue Profiles

Up to 12 distinct queue "profiles" may be defined using this page that may then be assigned to QoS queues as required. The queue profile determines how QoS queues with that profile assigned to them will behave.

Queue
This is the queue number that relates to the queues defined in the DCSP mappings page.

Minimum kbps
The value in this text box sets the minimum data transfer rate in kilobits/second that the router will try to attain for the queue.

Maximum kbps
The value in this text box sets the maximum data transfer rate in kilobits/second that the router will try to attain for this queue. This means that if the router determines that bandwidth is available to send more packets from a queue that has reached its Minimum kbps setting, it will send more packets from that queue until the Maximum kbps setting is reached.
Note that if the bandwidth on a queue should be restricted, setting the **Maximum kbps** value to the same as, or lower than the **Minimum kbps** value ensures that only the **Minimum kbps** setting will be achieved.

Maximum Packet Queue Length
The value in this text box specifies the maximum length of a queue in terms of the number of packets in the queue. Any packets received by the router that would cause the maximum length to be exceeded, are dropped.

WRED Minimum Threshold
The value in this text box specifies the minimum queue length threshold for using the WRED algorithm to drop packets. Once the queue length exceeds this value, the WRED algorithm may cause packets to be dropped.

WRED Maximum Threshold
The value in this text box specifies the maximum queue length threshold for using the WRED algorithm to drop packets. Once the queue length exceeds this value, the WRED algorithm will cause all packets to be dropped.

WRED Maximum Drop Probability (%)
The value in this text box sets the maximum percentage probability used by the WRED algorithm to determine whether or not a packet should be dropped when the queue length is approaching the WRED maximum threshold value.

Note:
If the length of a queue is less than the WRED minimum threshold value there is a 0% chance that a packet will be dropped. When the queue length is between the WRED minimum and maximum values, the % probability of a packet being dropped increases linearly up to the WRED maximum drop probability.

WRED Queue Length Weight factor
The value in this text box specifies a weighting factor to be used in the WRED algorithm when calculating the weighted queue length. The weighted queue length is based on the previous queue length and has a weighting factor that may be adjusted to provide different transmit characteristics. The actual formula used is:

new_length = (old_length * (1-1/2^n)) + (current_length * 1/2^n)
Small weighting factor values result in a weighted queue length that moves quickly and more closely matches the actual queue length. Larger weighting factor values result in a queue length that adjusts more slowly. If a weighted queue length moves too quickly (small weighting factor), it may result in dropped packets if the transmit rate rises quickly but will also recover quickly after the transmit rate tails off. If a weighted queue length moves too slowly (large weighting factor), it will allow a burst of traffic through without dropping packets, but may result in dropped packets for some time after the actual transmit rate drops off. The weighting factor should be selected carefully to suit the type of traffic using the queue.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
qprof	n	minkbps	0 - 2147483647	Minimum kbps
qprof	n	maxkbps	0 - 2147483647	Maximum kbps
qprof	n	qlen	0 - 2147483647	Maximum Packet Queue Length
qprof	n	minth	0 - 2147483647	WRED Minimum Threshold
qprof	n	maxth	0 - 2147483647	WRED Maximum Threshold
qprof	n	mprob	0 - 100	WRED Maximum Drop Probability (%)
qprof	n	wfact	0 - 2147483647	WRED Queue Length Weight factor

Command line examples.

To display a queue profile, enter the following command:

gqprof <instance> ?

Where <*instance*> is the number of the queue profile to be displayed.

To change the value of a parameter, use the following command:

qprof <instance> <parameter> <value>

To set the maximum throughput for queue profile 5 to 10kbps, enter the following command:

qprof 5 maxkbps 10

Timebands

Configuration – Network > Timebands

Digi TransPort routers support "Time Bands" which are used to determine periods of time during which PPP interfaces allowed or prevented from activating. For example, a router in an office could be configured so that the ADSL PPP interface is only raised on weekdays. Time Bands may only be applied to PPP instances.

Time Bands are specified by a series of "transition" times. At each of these times routing is either enabled or disabled. The default state for a Time Band is **On** which means that PPP instances that are associated with unconfigured Time Bands will operate normally. The router supports four Time Band configurations.

Note:
An entry is made in the event log whenever a Time Band transition occurs.

Whether or not Time Bands are enabled for a particular PPP instance is controlled by the settings in a table having the following columns:

Interface
This column simply lists the available PPP instances.

Enable
This column contains checkboxes, each checkbox controls whether or not Time Bands are enabled for the PPP instance in the left-hand column of the row. Check the checkbox to enable Time Bands for the associated PPP instance.

Timeband
This drop-down list selects which of the four available Time Band instances should be associated with the PPP instance.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ppp	n	tband	0 - 3	Timeband

The default state of this parameter is blank.

Timeband n

Configuration – Network > Timebands> Timeband n

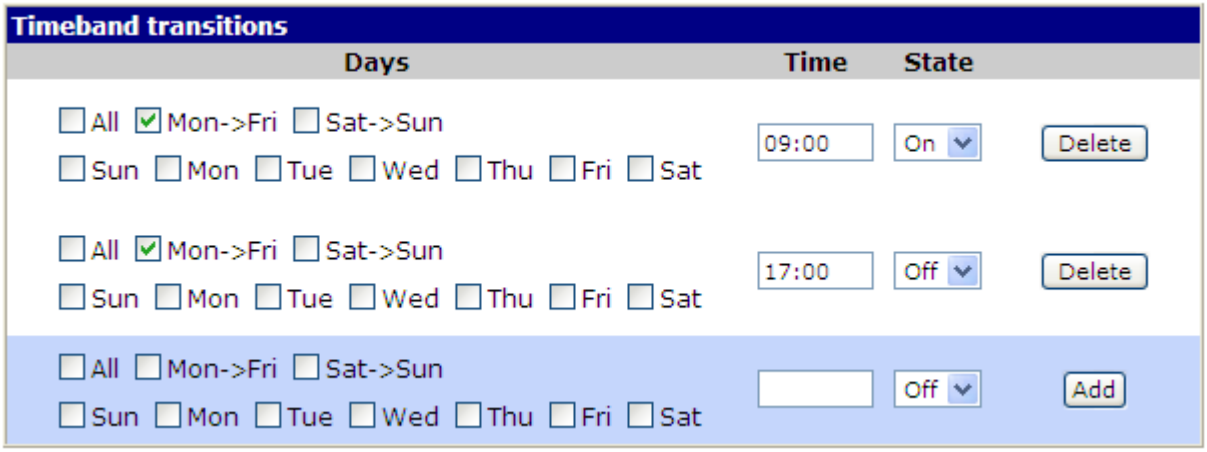
These four pages each control the configuration of one Time Band instance. Configuration is controlled by a table, having the parameters described below. Up to ten transitions may be configured.

Days
There is a selection of checkboxes in this column which are used to select which days of the week the Time Band transitions apply to. Days may be selected individually or in groups for convenience. So, for instance, to select all the days of the week, check the "**All**" checkbox. To select the weekend only, check the "**Sat->Sun**" checkbox. To select weekdays only, check the "**Mon->Fri**" checkbox.

Time
The value in this text box is the transition time. This is specified in 24-hour format with a colon separator between the hours and minutes.

State
This drop-down list selects the routing state which can be **On** or **Off**. (For convenience, the state of this parameter toggles for each new addition so if an on transition is configured, the default state for the next addition will be **Off**).

The following screenshot shows a PPP instance configured so that routing is allowed on weekday from 09:00 to 17:00. Clicking the **Add** button adds the entry into the table. Once an entry has been added to the table, it may be removed by clicking the associated **Delete** button. As mentioned previously, this Time Band instance is activated by navigating to the associated PPP Time Band (previous page) configuration page and clicking the Enable checkbox, or by entering the equivalent command line command.



Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
tband	0 - 3	days	ALL,MF,Mon, Tue,Wed,Thu,Fri,S at,Sun	Days
tband	0 - 3	time	HH:MM	Time
tband	0 - 3	state	OFF,ON	State

Command format:

tband <instance> <days#> <days>

tband <instance> <time#> <time>

tband <instance> <state#> <on|off>

To specify multiple days, separate the days with a comma, e.g. Mon,Wed,Fri. The abbreviation “MF” is used to specify Monday to Friday**.**

Example commands.

To allow PPP routing only on weekdays between 9:00 a.m. and 5:30 p.m. enter the following commands:

tband 0 days 0 mf

tband 0 time0 9

tband 0 state0 on

tband 0 days1 mf

tband 0 time1 5:30

tband 0 state1 off

Advanced Network Settings

Configuration – Network > Advanced Network Settings

The settings described in this web page are "advanced" in the sense that in the vast majority of configurations and implementations they should not require changing.

Secondary IP Address a.b.c.d
The value in this text box assigns an additional IP address to the router that is not associated with any particular interface. The router will respond directly to incoming traffic for this address, i.e. it will not attempt to onward route any IP packets for this address.

When connected to a Serial interface using TCP

Advertise an MSS of n bytes
The value in this text box sets the maximum segment size used/advertised by an asynchronous serial port connected to TCP sockets.

Use a Rx Window size of n bytes

The value in this text box sets the Rx window size used/advertised by an asynchronous serial port connected to TCP sockets.

Default SSL version for outgoing connections
This drop-down menu box selects which version of the SSL protocol to use in the "tcpdial" command. The options are:

- Auto, which allows the server to select the version.
- TLSv1 only
- SSLv2 only
- SSLv3 only.

Some servers are configured to work with a particular version, and unless this version is specifically requested, the connection attempt will fail.

Maximum DNS response cache time

This specifies the maximum time (in seconds) that the unit will cache negativeve DNS responses for. The maximum time to live for positive DNS responses remains at 300 seconds.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
cmd	n	sec_ip	Valid IP address	Secondary IP address a.b.c.d
sockopt	n	asymss	0 - 2147483648	When connected to a serial interface using TCP Advertise an MSS of n bytes
sockopt	n	asyrxwin	0 - 2147483648	Use a Rx Window size of n

Entity	Instance	Parameter	Values	Equivalent Web Parameter
				bytes
sockopt	n	sslver	0 – 3 0 = Auto 1 = TLSv1 2 = SSLv2 3 = SSLv3	Default SSL version for outgoing connections
ip	o	maxdnscache	Seconds (Default 300)	Maximum DNS response cache time

Socket Settings

Default source IP address interface x,y
The values in these two text boxes define the interface (None,PPP,ETH) and the instance number of the interface to use as a source address for IP when not using the interface that the socket was created on.
The router creates general-purpose sockets automatically when the controlling application requests them. As, for example, when TPAD calls are made over IP or XOT. Normally, the source address used by the socket will be that of the outgoing interface (usually PPP). However, for some applications such as when setting up a VPN, it may be necessary to specify that the socket uses a different source address such as that of the local Ethernet port. This parameter is used to specify the interface from which the source address should be derived.

Note:
Even when this parameter is not configured, the IP address from the interface on which the socket was created will be used. The source address specified in this parameter will only be used if it will cause the traffic to match an Eroute and therefore be sent using IPsec or GRE.

Connect Timeout s seconds
The value in this text box is used to specify the amount of time after which a TCP socket may remain idle before being closed. If the value is set to 0 the socket may remain open indefinitely.

TCP socket inactivity timer s seconds
The value in this text box specifies the maximum period of inactivity (in seconds) that may occur before and open TCP/IP socket is closed. The default value is 300 seconds (five minutes) and should not normally require altering.

TCP socket keep-alive s seconds
The value in this text box specifies the amount of time (in seconds) between sending “keep-alive” messages over open TCP connections. The purpose of these messages is to prevent a connection from closing even when no data is being transmitted or received. The default value of this parameter is zero which disables keep-alive messages.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
sockopt	n	gp_ipent	0,PPP,ETH	Default source IP address interface x,y
sockopt	n	gp_ipadd	Valid interface number	Default source IP address interface x,y

Entity	Instance	Parameter	Values	Equivalent Web Parameter
sockopt	n	sock_connto	0 - 2147483648	Connect Timeout s seconds
sockopt	n	sock_inact	0 - 2147483648	TCP socket inactivity timer s seconds
sockopt	n	sock_keepact	0 - 2147483648	TCP socket keep-alive s seconds

XOT Settings

Default source IP address interface x,y
The values in these two text boxes specify the interface (None,PPP,ETH) and instance number of that interface that IP address that XOT sockets should use instead of the interface that the socket was created on.

Note:
Even when this parameter is not configured, the IP address from the interface on which the socket was created will be used. The source address specified in this parameter will only be used if it will cause the traffic to match an Eroute and therefore be sent using IPsec or GRE.

NB of XOT listening sockets
The value in this text box specifies the maximum number of XOT sockets available. This may be used to reduce the number of XOT sockets in order to free up more general-purpose sockets for other purposes. The default value of 0 enables the maximum number of XOT sockets available.

Maximum ACK time for XOT data
The value in this text box sets the maximum time allowance for a remote unit to acknowledge TCP data transmitted by a unit's socket. If this timer expires, the socket is aborted. The default value of 0 disables the timer.

Note:
There is no requirement for the remote unit to acknowledge received data immediately, therefore setting this parameter to too small a value is not recommended. Some stacks delay sending TCP ACKs in order that they can be incorporated with data sent by the application.

Do not deactivate outgoing XOT sockets when interface disconnects
When checked, this checkbox sets outgoing XOT sockets not to close when the interface they are using disconnects.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
sockopt	n	xot_ipent	Valid interface type, ETH, PPP	Default source IP address interface x,y
sockopt	n	xot_ipadd	Valid interface number	Default source IP address interface x,y
sockopt	n	xot_listens	0 - 2147483648	NB of XOT listening sockets
sockopt	n	xot_maxack	0 - 2147483648	Maximum ACK time for XOT data

Backup IP Addresses

This page contains a table that is used to specify alternative IP addresses to use when the router fails in an attempt to open a socket. These addresses are used only for socket connections that originate from the router and are typically used to provide back-up for XOT connections, TANS (TPAD answering) connections or any application in which the unit is making outgoing socket connections.

When a backup address is in use, the original IP address that failed to open is tested at intervals to check if it has become available again. Additionally, at the end of a session, the unit will remember when an IP address has failed and use the backup address immediately for future connections. When the original IP address becomes available again, the router will automatically detect this and revert to using it.

The table has the following four column headings:

IP Address a.b.c.d
This text box should contain the original IP address to which the back-up address relates.

Backup IP address a.b.c.d
This text box should contain the backup address to try when the router fails to open a connection to the previous IP address.

Retry Time s (seconds)
This text box contains the length of time (in seconds) that the router will wait between checks to see if a connection can be made to **IP Address**.

Try Next
In the case that a connection to the primary IP address has just failed, this text box determines whether a connection to the backup IP address should be attempted immediately or when the application next attempts to open a connection. When checked, the socket will attempt to connect to the backup IP address immediately after the connection to the primary IP address failed and **before** reporting this failure to the calling application, e.g. TPAD. If the backup is successful this means that the application will not experience any kind of failure even though the router has connected to the backup IP address.
When unchecked, the socket will report the failure to connect back to the calling application immediately after the connection to the primary IP address has failed. The router will not try to connect to the backup IP address at this stage. The next time that the application attempts to connect to the same IP address, the router will instead, automatically connect to the backup IP address.

As is usual for these tables, the Add button and Delete button are used to add and delete entries to and from the table respectively.

Send “Backup IP” system messages to IP Address: a.b.c.d
The IP address in this text box specifies the destination to which system messages notifying of the unavailability of an IP address should be sent. This allows the router to send UDP messages to other routers to notify them that an IP address has become available/unavailable. Devices that receive the IP address available/unavailable messages Will search their own backup IP address tables for the IP addresses indicated and tag those addresses as available/unavailable as appropriate.

Chaining IP Addresses

It is possible to chain backup IP addresses by making multiple entries in the table.
For example, if the backup IP address for the original IP address appears as the IP address in the next row, along with a new backup IP address for that IP address, then when, the original IP address becomes unavailable, the router will try the backup IP address and if

that is unavailable, the router will try its backup IP address and so on. To make this example more concrete, say the original IP address is 192.168.0.1 with a backup IP address of 192.168.0.2, then setting the IP address in the next row to 192.168.0.2 with a backup IP address of 192.168.0.3 will cause the router to try all these IP addresses in succession.

Note:
The length of time that it takes for a connection to an IP address to fail is determined by the Connect timeout parameter on the ***Configuration – Network > Advanced Network Settings > Socket Settings*** web page.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ipbu	n	IPaddr	Valid IP address a.b.c.d	IP Address a.b.c.d
ipbu	n	BUIPaddr	Valid IP address a.b.c.d	Backup IP Address a.b.c.d
ipbu	n	retrysec	0 - 2147483648	Retry Time s (seconds)
ipbu	n	donext	OFF,ON	Try Next
sarsys	0	dest	Valid IP address a.b.c.d	Send “Backup IP” system messages to IP address a.b.c.d

Legacy Protocols

Configuration – Network > Legacy protocol

Older protocols that existed before TCP/IP became dominant are often referred to as legacy protocols. Examples of legacy protocols are X.25, SNA and LAPB.

Digi TransPort routers are capable of connecting to legacy networks such as X.25. They are also capable of simulating a legacy network so that equipment that in the past would have connected to a legacy network can connect to the Digi TransPort router instead. Thus old equipment can be connected to modern networks such as HSUPA.

The ***Configuration – Network > Legacy protocol*** menu has the following sub-menu options:

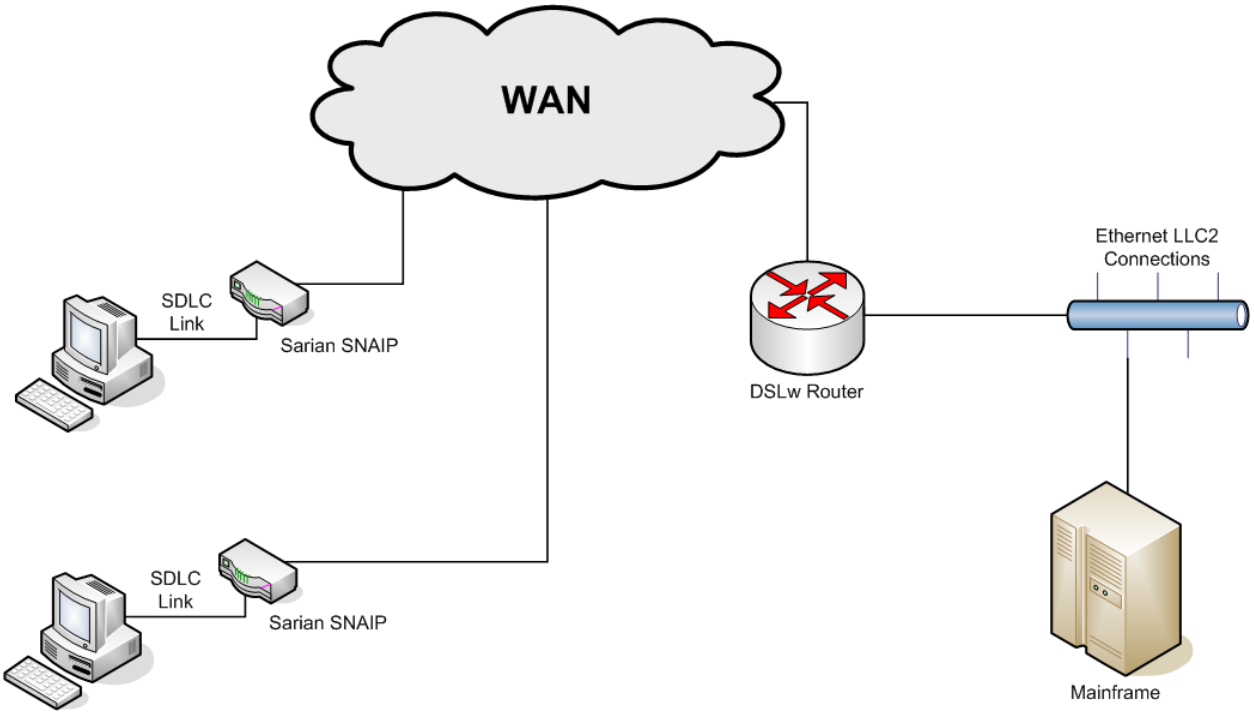
- Legacy Protocols TPAD
- X.25
- MODBUS

SNA over IP

Configuration – Network > Legacy protocol> SNA over IP

The unit is capable of sending Systems Network Architecture (SNA) traffic over TCP/IP, using the DLSw protocol, this is often called SNAIP. The unit is also capable of sending HDLC traffic over TCP/IP.

SNA uses Synchronous Data Link Control (SDLC) which is an unbalanced mode in which there is one master station and 1 or more secondary stations. Each secondary station owns a station address and can only respond when this address has just been polled by the master. A typical scenario is shown in the diagram below:



SNAIP 0

Configuration – Network > Legacy protocol> SNA over IP> SNAIP 0

Description
This parameter allows you to enter a name for this SNAIP instance, to make it easier to identify.

Send SNAIP traffic over interface
This setting determines which physical interface is to be used for carrying SNAIP data. This can be set to either “ISDN”, “Serial Port” or “SharedPort”. If “ISDN” is selected then SNAIP data is carried over the ISDN BRI physical interface. By selecting “Serial Port”, SNAIP data can be routed to either serial “Port 0” or serial “Port 1“ (operating in synchronous mode). To configure Port 0 or Port 1 for synchronous operation refer to the ***Configuration - Network > Interfaces > Serial > Serial Port x > Sync Port x***.

If "Shared Port" is selected, the drop down list next to “Shared Port” specifies the SNAIP instance that has sync port configured. When sync port sharing is enabled only one SNAIP instance can currently own the sync port. Other SNAIP instances however can share this sync port in the event that there is more than one terminal residing on a multi-drop sync line In this situation with multiple terminals, each terminal station will operate a DLSw state independently of all other stations.

The SNAIP parameter "Priority" is used to select the SNAIP instance to use when more than one is available; the highest number being given preference.

As an example consider that 4 SNAIP instances to all share sync port 0. To do this, configure SNAIP 0 in the usual way on "PORT 0" and then configure SNAIP instances 1,2 & 3 to use "SharedPort" and “Sync Port from SNAIP 0”

Use protocol
This parameter sets the appropriate protocol for the interface. Choose “LAPB”, “SNA” for SDLC or “RAW” for raw mode in which all L2 frames are transmitted and received. You can also choose “RAW_NOHDR” for raw mode with no DLSw headers.

Allow this unit to answer calls
If this parameter is set to “On”, the unit will answer incoming calls on the relevant LAPB session. To prevent the unit from answering incoming calls on this LAPB session set the option to “Off”. This setting is only relevant when the interface is set to ISDN.

Only accept calls with MSN ending with
This parameter provides the filter for the ISDN Multiple Subscriber Numbering facility. It is blank by default but when set to an appropriate value with answering calls parameter above enabled, it will cause the unit to answer incoming calls only to ISDN numbers where the trailing digits of the called number match the MSN value. For example, setting the MSN parameter to 123 will prevent the unit from answering any calls to numbers that do not end in 123. This setting is only relevant when the interface is set to ISDN.

Only accept calls with sub-address ending with
This parameter provides the filter for the ISDN sub-addressing facility. It is blank by default but when set to an appropriate value, with answering calls parameter above enabled, it will cause the unit to answer incoming ISDN calls only where the trailing digits of the sub address called match the Sub-address value. For example, setting the Sub-address to 123 will prevent the unit from answering any calls where the sub-address called does not end in 123. This setting is only relevant when the interface is set to ISDN.

Assume station exists (Do not send TEST frames)
When this parameter is enabled TEST frames are not transmitted and the TEST response is not expected. Instead the unit assumes the station exists and proceeds with the protocol as if the DLSw has received the TEST response.

Toggle DCD output each time the DLSw protocol enters the DISCONNECTED state
When this parameter is set to “On”, the DCD (Data Carrier Detect) output will turn off briefly each time the DLSw protocol enters the DISCONNECTED state. Thus any attached equipment that needs to will see signals changing state.

Sync port should not send or receive data when WAN link is down
This parameter causes the Sync port to be deaf and dumb (and have DCD low) while the connection with the WAN is down. This is so that some terminals don't get too excited just because L2 is up and think everything else should be working (and go into a management error state).

SNA Parameters

Configuration – Network > Legacy protocol> SNA over IP> SNAIP 0> SMA Parameters

Router to be Master on an unbalanced link

Enable this parameter if this unit is to be the Master in an unbalanced link, or “Off” if the unit is to be a secondary station.

Polling Response Time
The poll time in milliseconds (if the unit is the master in an unbalanced link).

Polling Stations Addresses
This parameter lists the station addresses on the data link as a comma-separated list of hex values (e.g. “c1,d1” for station addresses 0xc1 & 0xd1). This parameter is only applicable in SNA mode.

SAPs
This parameter contains a list of SAP values which correspond to the station addresses.

DSAPs(blank=default)
This is the Destination SAP value, if left blank the SAP value above is used.

Send Null XID (XID with no Data)
When this parameter is set to “On” a null XID SSP message will be sent when the unit has just received or sent a REACH ACK SSP message.

Send XID with Data
This parameter is a hex string to define binary data and defines an XID SSP message that would be sent in response to a XIDFRAME SSP message being received.

Tx Turn Around Time
This parameter specifies the time in milliseconds between receiving a frame from an outstation and transmission back to the same station. If this parameter is set to “0” this is disabled and the Digi can respond immediately. The minimum non-zero value is 10ms.

Mode
This parameter is used to define the mode in balanced links. In unbalanced links (like SNA/SDLC) the mode is defined by being master or the station, but for balanced links (like HDLC).

N400 counter
This is the standard LAPB retry counter. The default value is 3 and it should not normally be necessary to change this.

RR Timer
This is a standard LAPB/LAPD “Receiver Ready” timer. The default value is 10,000ms (10 seconds) and it should not normally be necessary to change this.

T1 timer
This is a standard LAPB timer. The default value is 1000 milliseconds (1 second) and under normal circumstances, it should not be necessary to change it.

T200 timer
This is the standard LAPB re-transmit timer. The default value is 1000 milliseconds (1 second) and under normal circumstances, it should not be necessary to change it.

Window Size
This parameter is used to set the X.25 window size. The value range is from 1 to 7 with the default being 7.

Disconnect link if there has been no activity for x seconds
This parameter may be used to specify the length of time (in seconds) before the link is disconnected if there has been no activity. If this parameter is zero or not specified, then the inactivity timer is disabled. It is useful to set this to a short period of time (say 120 seconds) when an LAPB instance is being used over ISDN. This timer can be used as a

backup hang-up timer thus saving ISDN call charges. When LAPB is being used on a synchronous port, this parameter should normally be set to 0.

SSP (WAN) Parameters

Configuration – Network > Legacy protocol> SNA over IP> SNAIP 0> SSP (WAN) Parameters

Virtual MAC Address
Virtual MAC address. The host uses MAC addresses and SAP values as the addressing values to discriminate between circuits (in much the same way as an IP address & TCP port define an addressing point for a TCP socket). This is the MAC address that is reported as part of the DLSw protocol.

Virtual MAC Address of Peer
The Virtual MAC address of the peer.

IP address of the Peer DLSw unit
The IP address of the peer DLSw unit.

Listen on Port
The read IP port. The TCP socket SNAIP listens on.

Use Port x if this unit starts the DLSw protocol
The write IP port. This TCP socket will be opened by the unit if it needs to start the DLSw protocol.

Use interface for source IP address
Setting this parameter to a “PPP” or “ETH” instance will cause the source address used by this SNAIP instance to match that of the Ethernet or PPP interface specified.

Close TCP connection if it is idle for x secs
This specifies the maximum period of inactivity (in seconds) that may occur before an open TCP/ IP socket is closed. The default value is 300 seconds (5 minutes) and should not normally require altering.

DLSw Ver
This parameter controls the DLSw version to be used. Set to 0 (default) for version 1, set to 2 for version 2.

DLSw Role
When this parameter is set to “Active”, and the unit is in SNA mode, then this DLSw switch will actively connect to the remote DLSw switch.

DLSw Window
This parameter is used to set the DLSw window size. The value range is from 10 to 100 with the default being 20.

UDP Capable
This controls the UDP transmission of DLSw SSP packets. Reception is always enabled for version 2 support. If set to “OFF”, the state transitions occur just like DLSw version 1 but the Digi will indicate it is version 2 capable.

Use 1 socket
When this parameter is set to “On” then only one socket is used for both read and write data. This is useful if the unit is behind a NAT box and incoming connections are not possible. This parameter can also be set to “Compatible”, in which mode both sockets are open to start with and then after a negotiation one of the sockets is dropped.

Include MAC Exclusivity Capability
On or Off. Set this parameter to "On" in order to include the MAC exclusivity value in the capabilities exchange message.

MAC Exclusivity Value
See above.

Ignore unsolicited response frames
When this parameter is enabled, the unit will ignore unsolicited response frames.

Wait for Contact before progressing to CONNECT PENDING state
During the DLSw negotiation phase and when XID messages are being exchanged this parameter controls which end sends the "CONTACT" message. Normally this would be off in which case this unit would send the "CONTACT" message, but if this parameter is set we would not send this message but instead wait for it to be sent to us before progressing in the DLSw state machine.

Make immediate connection attempts before backing off
This parameter defines the number of successive connection attempts before backing off for the number of seconds (default 30) defined in the "Backoff for x seconds" parameter. This backoff might be necessary in the case where a servers is behind a firewalls that detects too many successive connection attempts in a certain time frame.

Backoff for x seconds before attempting to connect again
When backing off because of too many failed consecutive connection attempts this parameter defines the time in seconds that we should remain idle for before attempting another connection.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snaip	x	l1iface	ISDN, Port, SharedPort	Send SNAIP traffic over interface
snaip	x	l1nb	0 – 255 (Select LAPB, Port or SharePort instance)	Send SNAIP traffic over interface
snaip	x	protocol	LAPB, SNA, RAW, RAW_NOHDR	Use protocol
snaip	x	ans	1 = enabled, 0 = disabled	Allow this unit to answer calls
snaip	x	msn	text	Only accept calls with MSN ending with
snaip	x	sub	text	Only accept calls with sub-address ending with
snaip	x	autocontact	1 = enabled, 0 = disabled	Assume station exists (Do not send TEST frames)
snaip	x	dcd_toggle	1 = enabled, 0 = disabled	Toggle DCD output each time the DLSw protocol enters the DISCONNECTED state
snaip	x	l1oos	1 = enabled, 0 = disabled	Sync port should not send or receive data when WAN link is down

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snaip	x	master	1 = enabled, 0 = disabled	Router to be Master on an unbalanced link
snaip	x	pollresp	0 - 2147483647	Polling Response Time
snaip	x	stations	text	Polling Stations Addresses
snaip	x	saps	text	SAPs
snaip	x	dsaps	text	DSAPs(blank=default)
snaip	x	send_xid_null	1 = enabled, 0 = disabled	Send Null XID (XID with no Data)
snaip	x	xid_data	text	Send XID with Data
snaip	x	turntxtim	0 - 2147483647	Tx Turn Around Time
snaip	x	dtemode	1 = DTE, 0 = DCD	Mode
snaip	x	n400	0 - 255	N400 counter
snaip	x	tnoact	1000 - 60000	RR Timer
snaip	x	t1time	1 - 60000	T1 timer
snaip	x	t200	1 - 60000	T200 timer
snaip	x	window	1 - 7	Window Size
snaip	x	tinact	0 - 3000	Disconnect link if there has been no activity for x seconds
snaip	x	vmac	Text (valid MAC address)	Virtual MAC Address
snaip	x	peervmac	Text (valid MAC address)	Virtual MAC Address of Peer
snaip	x	IPaddr	Text (valid IP address)	IP address of the Peer DLSw unit
snaip	x	r_IPport	0 - 65535	Listen on Port
snaip	x	w_IPport	0 - 65535	Use Port x if this unit starts the DLSw protocol
snaip	X	srcipent	auto, eth, ppp	Use interface for source IP address
snaip	x	srcipadd	0 - 255	Use interface for source IP address
snaip	x	sock_inact	0 - 2147483647	Close TCP connection if it is idle for x secs
snaip	x	ver	0 - 2	DLSw Ver
snaip	x	passive	0 = active, 1 = passive	DLSw Role
snaip	x	dlswwindow	1 - 100	DLSw Window
snaip	x	udp_cap	1 = enabled, 0 = disabled	UDP Capable
snaip	x	use1sock	On, Off, Compatible	Use 1 socket
snaip	x	inc_mac_exc	1 = enabled, 0 = disabled	Include MAC Exclusivity Capability
snaip	x	mac_exc_val	0 - 1	Mac Exclusivity Value

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snaip	x	iunsolresp	1 = enabled, 0 = disabled	Ignore unsolicited response frames
snaip	x	waitforcontact	1 = enabled, 0 = disabled	Wait for Contact before progressing to CONNECT PENDING state
snaip	x	con_attempts	0 - 2147483647	Make immediate connection attempts before backing off
snaip	x	con_boff_time	0 - 2147483647	Backoff for x seconds before attempting to connect again

Forcing SNAIP to use a specific instance

If several SNAIP instances are sharing an ASY port, a switchover to a specific instance can be initiated by issuing "**snasw x**". Where x is the SNAIP instance number, this instance must be available to go online or this command will fail.

To revert back and use the default instance, issue the "**snadis x**" command. Normal priorities will be used to determine which SNAIP instance gets to use the SYNC port.

Legacy Protocols TPAD

Configuration – Network > Legacy protocol> TPAD

TPAD is a simplified version of the X.25 PAD specification that is commonly used for carrying out credit-card clearance transactions. Digi units support the use of TPAD over:

ISDN B and D-channels

TCP

UDP

SSL

XoT

Automatic back-up between any two of these "layer 2 interfaces" or "transport protocols" is supported.

For further information on using TPAD please refer to Digi technical support and ask for a copy of "TG2 - Introduction to TPAD and X.25".

Legacy Protocols TPAD n

Configuration – Network > Legacy protocol> TPAD > TPADn

Use TPAD over interface
This section is used to select whether the TPAD instance will use ISDN B-channel X.25, ISDN D-channel X.25, TCP, VXN or SSL as the transport protocol. For ISDN D-channel operation, ensure that the "LAPD" option is selected. For ISDN B-channel operation or operation through a synchronous port, select "LAPB". In the case of LAPB and LAPD it is also possible to specify an interface number. This parameter specifies which LAPB or LAPD instance to use for the relevant TPAD instance. Select "0" or "1" for LAPB or "0" or "1" for LAPD. When using LAPB with ISDN this parameter may be set to "255", which means use any free LAPB instance. This is useful when more than 2 POS terminals are connected to the router and the acquirer does not support multiple Switched Virtual Circuits (SVCs) on a single B-Channel. A value of 254 will use an available LAPB instance but will use the same

ISDN B channel if two calls are attempted to the same ISDN number at the same time. (All services that the POS terminals may dial must support multiple SVCs if using the setting 254.)

Use backup interface
This section is used to specify a backup interface that will be used automatically if the call to the primary interface fails. Note that the primary interface will be tried first for every new call attempt.

ISDN settings

Use number x to make outgoing ISDN calls
This parameter may be used to specify an ISDN number. This is used in cases where no ISDN number is provided with the ATD command when making an outgoing call.

Use prefix x
This parameter is used to specify a dialling code that the unit will place in front of the telephonenumber that is issued by the terminal in the ATD command. For example, if the Prefix # was set to 0800 and the number specified by the terminal in the ATD command was 123456, the actual number dialled by the unit would be 0800123456.

Remove prefix x from number in ATD command
This parameter is used to specify a dialling prefix that is normally inserted by the terminal in the ATD command that is removed by the unit before dialling takes place. For example, if the Prefix removal # was set to 0800 and the terminal issued an ATD command containing 0800123456 then the actual number dialled by the unit would be 123456.

Use suffix x
The Suffix # parameter may be set to contain additional numbers that are dialled after the number specified by B-channel ISDN #. For example, if B-channel ISDN # was set to 123456 and Suffix # was set to 789, the actual number dialled would be 123456789.

On the main interface Deactivate LAPB session x seconds after TPAD X.25 call has been cleared
Once a TPAD X.25 call has been cleared, the unit will keep a LAPB instance active for the length of time set by this parameter. This is to allow further TPAD transactions to take place without having to make another ISDN call. The default value of 10 seconds should be acceptable for most applications. The value of 1 is a special value which means terminate layer 2 immediately the transaction is finished. (When the X.25 call is cleared.)

If you select LAPD as the TPAD layer-2 interface, this value will automatically be set to 0 to disable layer-2 deactivation. You may still override the 0 setting by entering a new value but note that most network service providers prefer that LAPD connections are not repeatedly deactivated.

On the backup interface Deactivate LAPB session x seconds after TPAD X.25 call has been cleared.
This is equivalent to the deactivation timer above but applies only to backup calls.

With X.25 over ISDN D-channel mode

Send X.25 RESTART packets
d

Delay the X.25 RESTART packets by x milliseconds
d

X.25 settings

Default X.25 Packet Size
This parameter specifies the default X.25 packet size to be used for TPAD transactions.

Use NUA
This parameter specifies the X.25 Network User Address to be used for outgoing X.25 calls if no NUA is specified in the call string.

Use NUI
This specifies the X.25 Network User Identifier to be used for outgoing X.25 calls if no NUI is specified in the call string.

LCN
The unit supports up to eight logical X.25/TPAD channels. In practice, the operational limit is determined by the particular service to which you subscribe (usually 4).
Each logical channel must be assigned a valid Logical Channel Number (LCN). The LCN parameter is the value of the first LCN that will be assigned for outgoing X.25 CALLs. The default is 1027. For incoming calls, the unit accepts the LCN specified by the caller.

LCN direction
This parameter determines whether the X.25 LCN used for outgoing TPAD calls is incremented or decremented from the starting value when multiple TPAD instances share one layer 2 (LAPB or LAPD), connection. The default is “DOWN” and LCNs are decremented, i.e. if the first CALL uses 1024, the next will use 1023, etc. Setting the parameter to “UP” will cause the LCN to be incremented from the start value.

On the backup interface

Use NUA
The LCN parameter is used to set the first LCN that will be used for the backup interface.

Use NUI
This specifies the X.25 Network User Identifier to be used for outgoing X.25 calls if no NUI is specified in the call string for the backup interface.

LCN
The LCN parameter is used to set the first LCN that will be used for the backup interface.

LCN direction
This parameter determines whether the LCN used for the backup X.25 interface is incremented or decremented from the starting value when multiple X.25 instances share a single layer 2 connection.

Report our NUA as n to the X.25 network
This is the NUA that the unit will report to the X.25 network as its own NUA when making a call. It is also known as the calling NUA. Often the X.25 network will override this NUA.

Call User Data
This specifies a text string that will be placed in the Call User Data field of an outgoing X.25 call request packet. Whether or not this information is required will depend on the X.25 host that you are connecting to. In most cases the information is not required.

X.25 calls

These setting control how transactions are sent to the host when TPAD is running in “direct mode”.

One per transaction
Only one transaction is allowed per call.

Allow consecutive transactions
Multiple transactions are allowed per X.25 call, but not until a response has been received from the host.

Allow concurrent transactions
Multiple transactions per X.25 call are allowed irrespective of whether a response has been received from the host.

Use ASCII character x as the delimiter character
This parameter specifies the character used to separate a main NUA from a backup NUA, and a main NUI from a backup NUI in an ATD command. The default value is the ASCII "!" character (decimal 33).

Forward mode time x milliseconds
If not framed with STX and ETX characters, can still have data formatted after this period.

Create an event when reply from X.25 host matches
This parameter can be used to generate a "Data Trigger" event (code 47) when the reply from the X.25 host contains the string specified in this parameter. It is possible to configure the unit to generate an email alert message when this event occurs. See "LOGCODES.TXT" for a complete list of events.

XoT/TCP settings

Connect to remote IP address
When the unit is configured for XOT or TCP socket mode, this parameter is used to specify the IP address of the host to which the TCP/XOT connection is made. Note that the transport protocol must be set to TCP.

Port
When making a TCP socket connection (i.e. the transport protocol has been set to TCP not XoT), this parameter must be used to specify the TCP port number to use.

IP length header
When making a TCP socket connection (i.e. the transport protocol has been set to TCP), setting this parameter to "On" will pre-pend the data sent to the host with a 2 byte length header. The 2 byte length header will not be included in the length calculation. When set to "8583 Ascii 4 byte", the IP length header will conform to the ISO 8583 format. When set to "On Inclusive" it will pre-pend a 2 byte length header and the calculation of the length will include the 2 bytes of the length header.

TPAD Settings

Use Terminal ID (TID)
The Terminal ID parameter can be used to insert or replace a Terminal ID in the APACS 30 string.

Replace TID provided by connected terminal with configured TID
When this check box is ticked, any Terminal ID provided by a connected terminal will be replaced by the ID set in the Use Terminal ID field above.

The TID will be become inactive in n seconds.
This specifies the time in seconds before the Terminal ID is considered inactive. Local authorisations may be configured to occur on active TIDs (terminal Ids), so this parameter defines how long a time (without transactions) must pass for a TID to change from active to inactive.

Use TID xxxxxxxxx with incoming APACS 50 polling calls

This parameter specifies the terminal ID to associate with this TPAD instance when answering an incoming APACS 50 polling call.

Use merchant Number
This parameter can be used to insert a merchant number into the APACS 30 string when the locally connected equipment does not transmit a merchant number.

Use Connect String
This parameter specifies a string to be sent to the user's terminal when an outgoing TPAD call has been connected, instead of the normal ENQ character. For example, this might be used to make a TPAD connection look like a PAD connection by specifying "CON COM" as the connect string.

The polling character set is c
This parameter is a string that specifies a character or set of characters to be treated as polling characters. The unit will respond to any of these characters using ACK. This parameter should normally be left blank.

Enable Message Numbering
When this check box is ticked the unit will override the message numbering of the local equipment and substitute its own message numbering in the APACS 30 data. This is useful when the locally connected equipment does not automatically increment the APACS 30 message number.

Disable Direct Mode
Enabling this setting will prevent the unit from automatically using Direct Mode (see below) when it receives an APACS 30 packet without any call set-up.

Boot to Direct Mode
Direct mode is a mode of operation whereby the unit automatically routes APACS 30 packets to their destination without the terminal having to perform any call control. If this parameter is set to "Yes", then the next time the unit is rebooted it will operate in direct mode. For Direct Mode to work you must set up the appropriate addressing information (e.g. Transport protocol, NUA, NUI, IP address etc). If this parameter is not enabled the unit will still try to use direct mode if it detects that it is required (due to the absence of call control information). This parameter can be used in certain cases where for some reason the unit cannot automatically determine whether or not to use direct mode.

Use response code n in "unable to authorise" message
This parameter only applies when the unit is operating in direct mode. In cases where the unit is unable to send the APACS 30 packet to the remote host, it replies to the terminal with an "unable to authorise" message. By default, this message contains a response code 05 which means declined. Entering a number for this parameter causes the unit to use that number in place of the default response code. A value of zero for this parameter prevents the unit from replying.

Clearing time n milliseconds
This parameter defines the clearing time in milliseconds that an X.25 call will be left "open" after receiving a response from the host. Each response from the host resets this timer.

Delay transmitting the APACS 30 string for x milliseconds after connecting to X.25 host
Setting this parameter will cause the unit to pause for the specified number of milliseconds in between successfully connecting to the remote X.25 host and transmitting the APACS 30 string.

Retransmit APACS 30 string if error detected

Ticking this check box will cause the unit to retransmit the APACS 30 string to the terminal if an error is detected. (e.g. no ACK received from terminal)

STX/ETX removal
Enabling “Del STX&ETX” will cause the unit to strip off the STX and ETX characters that normally surround the APACS 30 string before sending it to the host. Enabling “Del STX only” will cause it to strip of the STX character only.

Do not transmit ENQ characters
Under the TPAD protocol the ENQ character is normally used to indicate that a call has connected and that the TPAD terminal may proceed with the transaction. Enabling this parameter will prevent the router from transmitting ENQ characters to the TPAD terminal when a connection is made.

Delay sending ENQ characters to TPAD terminal for x milliseconds when a call has been connected
This parameter may be used to set the delay in ms from when the router first connects the call to when it transmits the ENQ to the terminal. By default there is no delay.

Wait for x milliseconds for an ACK before retransmitting the data
This parameter defines the time period the unit will wait for an ACK character to be received after sending data to the terminal. If an ACK character is not received within this time the data will be retransmitted. A value of “0” entered here will default to a delay of 1 second.

Transmit TPAD transactions directly in a Synchronous frame
When this check box is ticked TPAD transactions are transmitted without any “outer” protocol such as X.25, i.e. they are placed directly in a synchronous frame on ISDN. This sometimes referred to as HDLC by certain card acquirers.

Include LRC
The LRC (Longitudinal Redundancy Check) is a form of error checking that may be required by some TPAD terminals. When the Include LRC option is enabled the unit will check the LRC sent by the terminal and if it indicates a problem has occurred NAK the message. If this parameter is enabled but no LRC is sent by the terminal, the transaction will not be forwarded to the host.

Include LRC line
This parameter is normally disabled so that any LRCs received from a TPAD terminal will be removed before the transaction data is transmitted to the remote host. In most cases this is acceptable because the network will provide error correction and so the LRC is redundant. In some circumstances it may be necessary to enable this parameter so that the unit transmits the LRC to the remote host along with the transaction data.

Force parity when sending data to the terminal
When this parameter is enabled the unit will always use even parity when relaying data from a remote host to a locally connected TPAD terminal. To allow data to pass through without the parity being changed disable this setting.

Strip parity when sending data to the host
Enabling this parameter will cause the unit to remove any parity before sending the data to the host.

Force parity when sending data to the host
When this parameter is enabled the unit will always use EVEN parity when relaying data from the locally connected TPAD terminal to the remote host. To allow data to pass through without the parity being changed disable this setting.

Strip Trailing Spaces

When this parameter is enabled the TPAD instance will look at responses coming from the host and remove any trailing space characters from the end of the packet before relaying the data to the terminal. This may be necessary if the host system "pads out" responses with unnecessary spaces which can cause abnormal behaviour in some terminals.

Acknowledge TPAD data packets
This parameter causes the unit to acknowledge TPAD data packets from the terminal. This parameter should normally be enabled. Note that this parameter is only used if no polling characters (see above) are defined.

Convert leading STX character to SOH
Enabling this parameter will cause the unit to convert the leading STX character in a transaction to an SOH character.

Terminate TPAD call is EOT only
A TPAD call is normally terminated with a DLE EOT sequence. Some terminals only require the EOT character on its own. If this is the case then enable this parameter.

Clear TPAD call if there is no response to a TPAD transaction request for x seconds
This is the length of time in seconds that the unit will wait for a response to a TPAD transaction request before clearing the TPAD call.

Generate an event when a TPAD transaction takes longer than x seconds
Setting this parameter to a non-zero value causes the unit to generate an "Excessive Transaction Time" event (code 56) each time a TPAD transaction takes longer that the specified number of seconds. This could be used in conjunction with an appropriate Event Handler configuration to generate email alert messages or SNMP traps when TPAD transactions take longer than expected. See ***Configuration - Alarms > Event Logcodes*** for a complete list of events.

When the transaction time exceeds x milliseconds, increment the "SLA Exceptions" statistic
When the total transaction time exceeds the value (in ms) set in this parameter, the NB SLA exceptions statistic on the Diagnostics - Statistics > TPAD page is incremented. This statistic can be viewed on the CLI interface by entering the at\mibs=tpad.n.stats command, where n is the TPAD instance.

Clear the call x seconds after receiving a response
This parameter defines the time period for which the socket closing or the X.25 call clearing is delayed by after the TPAD session has finished. For example, if this parameter is set to 10 then 10 seconds after the TPAD session is finished (NO CARRIER is seen on the ASY TPAD port) the network call (X25 or TCP socket) is cleared. The number "1" is a special value. If set to the number "1" the call will be cleared immediately (not after 1 second).

If the terminal dial command specifies V.120 use PANS context x
This parameter is for advanced users only. It enables TPAD transactions to be carried out using the V.120 protocol ("ATDV" command). The parameter is used in conjunction with the Polling Answering Service (PANS), and identifies which PANS instance is to be used for an outgoing V.120 call. For this to work, the PANS instance must be bound to a Rate Adaption instance.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
tpad	n	l2iface	lapb, lapd, tcp, ssl, vxn	Use TPAD over interface
tpad	n	l2nb	0 – 255	Use TPAD over interface

Entity	Instance	Parameter	Values	Equivalent Web Parameter
tpad	n	ipmode	0=XOT, 1=raw TCP	Use TPAD over interface
tpad	n	bakl2iface	lapb, lapd, tcp, ssl, vxn	Use backup interface
tpad	n	bakl2nb	0 - 255	Use backup interface
tpad	n	bnumber	text (valid ISDN number)	Use number x to make outgoing ISDN calls
tpad	n	prefix	text (numeric)	Use prefix x
tpad	n	prefix_rem	text (numeric)	Remove prefix x from number in ATD command
tpad	n	suffix	text (numeric)	Use suffix x
tpad	n	tl2deact	0 - 10000	On the main interface Deactivate LAPB session x seconds after TPAD X.25 call has been cleared
tpad	n	baktl2deact	0 – 10000	On the backup interface Deactivate LAPB session x seconds after TPAD X.25 call has been cleared.
tpad	n	defpak	16,32,64,128,256,512,1024	Default X.25 Packet Size
tpad	n	nua	text	Use NUA
tpad	n	nui	text	Use NUI
tpad	n	lcn	1 - 4095	LCN
tpad	n	lcnup	1 = up, 0 = down	LCN direction
tpad	n	baknua	text	(Backup) Use NUA
tpad	n	baknui	numeric text	(Backup) Use NUI
tpad	n	baklcn	1 - 4095	(Backup) LCN
tpad	n	baklcnup	1 = up, 0 = down	(Backup) LCN direction
tpad	n	cingnua	numeric text	Report our NUA as n to the X.25 network
tpad	n	cud	text	Call User Data
tpad	n	samecall	0	One per transaction
tpad	n	samecall	1	Allow consecutive transactions
tpad	n	samecall	2	Allow concurrent transactions
tpad	n	delimchar	32 - 127	Use ASCII character x as the delimiter character
tpad	n	ftime	0 - 20000	Forward mode time x

Entity	Instance	Parameter	Values	Equivalent Web Parameter
				milliseconds
tpad	n	trig_str	text	Create an event when reply from X.25 host matches
tpad	n	IPaddr	IP address	Connect to remote IP address
tpad	n	iphdr	0=Off 1=On 2=8583 Ascii 4 byte	IP length header
tpad	n	termid	text	Use Terminal ID (TID)
tpad	n	dotermid	1 = enabled, 0 = disabled	Replace TID provided by connected terminal with configured TID
tpad	n	tid	text	Use TID xxxxxxxxx with incoming APACS 50 polling calls
tpad	n	merchnum	text	Use merchant Number
tpad	n	useconstr	1 = enabled, 0 = disabled	Use Connect String
tpad	n	constr	text	Use Connect String
tpad	n	pollchars	text	The polling character set is c
tpad	n	domsgnb	1 = enabled, 0 = disabled	Enable Message Numbering
tpad	n	disdir	1 = enabled, 0 = disabled	Disable Direct Mode
tpad	n	bdir	1 = enabled, 0 = disabled	Boot to Direct Mode
tpad	n	uaarc	0 - 99	Use response code n in "unable to authorise" message
tpad	n	clear_dirtime	0 - 60000	Clearing time n milliseconds
tpad	n	trandel	0 - 5000	Delay transmitting the APACS 30 string for x milliseconds after connecting to X.25 host
tpad	n	teretran	1 = enabled, 0 = disabled	Retransmit APACS 30 string if error detected
tpad	n	delstx	1 = enabled, 0 = disabled	STX/ETX removal
tpad	n	no_enq	1 = enabled, 0 = disabled	Do not transmit ENQ characters

Entity	Instance	Parameter	Values	Equivalent Web Parameter
tpad	n	tenqdel	0 - 5000	Delay sending ENQ characters to TPAD terminal for x milliseconds when a call has been connected
tpad	n	tackdel	0 – 10000	Wait for x milliseconds for an ACK before retransmitting the data
tpad	n	dsync	1 = enabled, 0 = disabled	Transmit TPAD transactions directly in a Synchronous frame
tpad	n	inclrc	1 = enabled, 0 = disabled	Include LRC
tpad	n	incllrc	1 = enabled, 0 = disabled	Include LRC line
tpad	n	fpar	1 = enabled, 0 = disabled	Force parity when sending data to the terminal
tpad	n	lrpar	1 = enabled, 0 = disabled	Strip parity when sending data to the host
tpad	n	lfpar	1 = enabled, 0 = disabled	Force parity when sending data to the host
tpad	n	strip_tspaces	1 = enabled, 0 = disabled	Strip Trailing Spaces
tpad	n	ackdat	1 = enabled, 0 = disabled	Acknowledge TPAD data packets
tpad	n	stx_2_soh	1 = enabled, 0 = disabled	Convert leading STX character to SOH
tpad	n	eot_only	1 = enabled, 0 = disabled	Terminate TPAD call is EOT only
tpad	n	tresp	0 – 1000	Clear TPAD call if there is no response to a TPAD transaction request for x seconds
tpad	n	texcess	0 – 100	Generate an event when a TPAD transaction takes longer than x seconds
tpad	n	tsla	0 – 3000	When the transaction time exceeds x milliseconds, increment the "SLA Exceptions" statistic
tpad	n	clear_time	0 - 2147483647	Clear the call x seconds after receiving a response
tpad	n	dialctx	0 - 255	If the terminal dial command specifies V.120

Entity	Instance	Parameter	Values	Equivalent Web Parameter
				use PANS context x

X.25

Configuration – Network > Legacy Protocol > X.25

The ***Configuration – Network > Legacy Protocol > X.25*** menu has the following sub-menu options:

- General
- LAPB
- NUI Mappings
- NUA / NUI Interface Mappings
- Calls Macros
- IP to X.25 Calls
- PADS n
- X.25 Settings
- IP Settings
- PADs
- X.25 PVCs

General

Configuration – Network > Legacy Protocol > X.25> General

This section contains some global X.25 settings.

When answering a X.25 call, use the addresses from CALL packet in the CALL CNF packet
When this setting is enabled when answering a call the called and calling addresses from the CALL packet are used in the X25 CALL CNF (call confirm packet) that the unit sends to answer the call. This setting can be enabled on a per “interface type” basis, (LAPD, LAPB or XoT)

Reset XOT PVC if the router is the Initiator
When this parameter is enabled the unit is responsible for resetting the links when an XOT PVC comes up. This parameter should only be set to “Off” when it is known that the responder will reset the links.

Reset XOT PVC if the router is the Responder
When this parameter is set to “On” the unit is responsible for resetting the links on XOT PVC links when it is the responder. The default for this parameter is “Off”.

Include length of header in IP length header

For all X.25 calls which include an IP header length indication (i.e. IP Length Header is set to “On” a TPAD or PAD, etc.) this parameter specifies whether the length indicated includes or excludes the length of the header itself.

By default it is “Off”, in which case the length of the header is NOT included in the value. For example, say we had one byte of data of value 67 to encode. Then “00 01 67” is the encoding if this parameter is set to “Off” as the length (00 01) is 1 because the length does not include the length of the header. When set to “On” the length of the IP header is included in the value, i.e. “00 03 67” is the encoding as the header bytes are included.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
X25gen	0	lapd_cnf_addr	1 = enabled, 0 = disabled	When answering a X.25 call, use the addresses from CALL packet in the CALL CNF packet. LAPD setting
X25gen	0	lapd_cnf_addr	1 = enabled, 0 = disabled	When answering a X.25 call, use the addresses from CALL packet in the CALL CNF packet LAPB setting
X25gen	0	xot_cnf_addr	1 = enabled, 0 = disabled	When answering a X.25 call, use the addresses from CALL packet in the CALL CNF packet XoT setting
X25gen	0	reset_xotpvc_ini	1 = enabled, 0 = disabled	Reset XOT PVC if the router is the Initiator
X25gen	0	reset_xotpvc_resp	1 = enabled, 0 = disabled	Reset XOT PVC if the router is the Responder
X25gen	0	en_incl_iphdr	1 = enabled, 0 = disabled	Include length of header in IP length header

LAPB > LAPB n

Configuration – Network > Legacy Protocol > X.25 > LAPB > LAPB n

LAPB (Link Access Procedure Balanced) is a standard subset of the High-Level Data Link Control (HDLC) protocol. It is a bit-oriented, synchronous, link-layer protocol that provides data framing, flow control and error detection and correction. LAPB is the link layer used by X.25 applications.

On Digi TransPort routers LAPB can be used over ISDN or over a synchronous serial port.

Use: Serial port Port x (in Synchronous Mode)
To use the LAPB instance over a synchronous serial port enable this setting and select a serial port number. To configure settings of the synchronous port such as speed and clock source navigate to ***Configuration - Network > Interfaces > Serial > Serial Port n > Sync Port n.***

Use: ISDN
Enable this setting to use LAPB over ISDN.

Mode DTE or DCE
Determines whether LAPB will behave as DTE (Data Terminal Equipment) or DCE (Data Circuit-terminating Equipment) in an X.25 protocol sense. (Physical DTE vs. DCE wiring cannot be changed by configuration.)

N400 Counter x
This is the standard LAPB retry counter. The default value is 3 and it should not normally be necessary to change this.

RR Timer x milliseconds
This is a standard LAPB "Receiver Ready" timer. The default value is 10,000ms (10 seconds) and it should not normally be necessary to change this.

T1 Timer x milliseconds
This is a standard LAPB timer. The default value is 1000 milliseconds (1 second) and under normal circumstances, it should not be necessary to change it.

T200 Timer x milliseconds
This is the standard LAPB re-transmit timer. The default value is 1000 milliseconds (1 second) and under normal circumstances, it should not be necessary to change it.

X.25 Window Size
This parameter is used to set the X.25 window size. The value range is from 1 to 7 with the default being 7.

Disconnect link if there has been no X.25 activity for x seconds
This parameter may be used to specify the length of time (in seconds) before the link is disconnected if there has been no X.25 activity. If this parameter is zero or not specified, then the inactivity timer is disabled.

Disconnect link if there has been no activity for x seconds
This parameter may be used to specify the length of time (in seconds) before the link is disconnected if there has been no activity. If this parameter is zero or not specified, then the inactivity timer is disabled. It is useful to set this to a short period of time (say 120 seconds) when a LAPB instance is being used over ISDN for example with TPAD. Should the POS device fail to instruct TPAD to hang up then this timer can be used as a backup hang-up timer thus saving ISDN call charges. When LAPB is being used on a synchronous port, this parameter should normally be set to 0.

Send X.25 Restart packet on receipt of SABM frame
This parameter can be set to "No" or "Immediate". When set to "Immediate", the LAPB instance will send an X.25 restart packet immediately on receipt of an SABM (Set Asynchronous Balanced Mode) frame. If the parameter is set to "No", then no X.25 restart is sent.

ISDN Parameters

Configuration – Network > Legacy Protocol > X.25> LAPB> LAPN n> ISDN Parameters

Allow this unit to answer calls
When this parameter is enabled this instance of LAPB will answer incoming ISDN calls.

Only accept calls from calling number ending with
This parameter provides the filter for the ISDN Multiple Subscriber Numbering facility. It is blank by default but when set to an appropriate value with "Allow this unit to answer calls" enabled it will cause the unit to answer incoming calls only to ISDN numbers where the trailing digits match the MSN value. For example, setting the MSN parameter to 123 will prevent the unit from answering any calls to numbers that do not end in 123.

Only accept calls with sub-address ending with
This parameter provides the filter for the ISDN sub-addressing facility. It is blank by default but when set to an appropriate value, with "Allow this unit to answer calls" enabled it will

cause the unit to answer incoming ISDN calls only where the trailing digits of the sub address called match the Sub-address value. For example, setting the Sub-address to 123 will prevent the unit from answering any calls where the sub-address called does not end in 123.

Keep ISDN LAPB link activated when user sends a DISC or X.25 PAD session terminated
When this parameter is enabled

Wait x milliseconds before attempting to establish the LAPB link after B-channel becoming active
This parameter sets the length of time (in milliseconds), that the LAPB instance will wait from an ISDN B-channel becoming active before attempting to establish a LAPB connection, i.e. the length of time for which the LAPB instance stays passive. The default is 0 as most ISDN networks allow CPE devices to initiate a LAPB link. If your ISDN network does not permit CPE devices to initiate the LAPB link you should set this parameter to a value that allows the network sufficient time to establish the LAPB link.

Use as x a calling party number when making ISDN calls
This is "Calling Line Identification". The unit will only answer calls from numbers whose trailing digits match what is entered in this field. The line the unit is connected to must have CLI enabled by the telecoms provider, and the calling number cannot be withheld.

Async Mux 0710 Parameters

Configuration – Network > Legacy Protocol > X.25> LAPB> LAPN n> Async Mux 0710 Parameters

For certain W-WAN modules LAPB is used to perform multiplexing of serial channels. If using LAPB for X.25 over ISDN or serial then these settings should be ignored. These settings should not be changed unless under the instruction of technical support.

Mux 0710 mode
When enabled configures the LAPB instance to be used for multiplexing of serial channels instead of X.25.

Mux mode
This setting controls the multiplexing mode.

DLC #
The data link channel number to use for this virtual ASY port.

ASY port
This is the physical ASY port over which to multiplex.

Virtual ASY port
This is the virtual ASY port number that this LAPB instance will multiplex over the physical port.

Entity	Instance	Parameter	Values	Equivalent Web Parameter
lapb	n	l1iface	port, isdn (use "port" for sync port)	Use: Serial port Port x (in Synchronous Mode)
lapb	n	l1nb	0,1	Use: Serial port Port x (in Synchronous Mode) 0 for "Port 0", 1 for "Port 1"

Entity	Instance	Parameter	Values	Equivalent Web Parameter
lapb	n	l1iface	port, isdn (use "isdn" for ISDN)	Use: ISDN
lapb	n	dtemode	DTE/DCE mode: 0=DTE 1=DCE	Mode DTE or DCE
lapb	n	N400	1 - 255	N400 Counter x
lapb	n	tnoact	1000 - 60000	RR Timer x milliseconds
lapb	n	t1time	1 - 60000	T1 Timer x milliseconds
lapb	n	t200	1 - 60000	T200 Timer x milliseconds
lapb	n	Window	1 - 7	X.25 Window Size
lapb	n	tinactx25	0 - 3000	Disconnect link if there has been no X.25 activity for x seconds
lapb	n	tinact	0 - 3000	Disconnect link if there has been no activity for x seconds
lapb	n	restartact	1 = enabled, 0 = disabled	Send X.25 Restart packet on receipt of SABM frame
lapb	n	ans	1 = enabled, 0 = disabled	Allow this unit to answer calls
lapb	n	msn	text	Only accept calls from calling number ending with
lapb	n	sub	text	Only accept calls with sub-address ending with
lapb	n	ptime	0 - 60000	Wait x milliseconds before attempting to establish the LAPB link after B-channel becoming active
lapb	n	cli	text	Only answer calls from numbers whose trailing digits match
lapb	n	mux_0710	1 = enabled, 0 = disabled	Mux 0710 mode
lapb	n	mux_mode	0 = Basic, 1 = Error Recovery	Mux mode
lapb	n	dlc	0 - 63	DLC #
lapb	n	asyport	0 - 255	ASY port
lapb	n	virt_async	0 - 255	Virtual ASY port

NUI Mappings

Configuration – Network > Legacy Protocol > X.25> NUI Mappings

When a TPAD call is taking place the attached terminal sometimes only specifies an “NUI” (Network User ID) to call. If the X.25 network requires an NUA instead of an NUI to determine the destination of a call then the NUI Mappings table can be used to convert an NUI to an NUA.

If a TPAD call specifies a call in which the NUI matches an entry the call actually placed on the network will contain the respective NUA and no NUI.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
nuimap	n	nua	text	Maps to NUA
nuimap	n	nui	text	NUI

NUA / NUI Interface Mappings

Configuration – Network > Legacy Protocol > X.25> NUI / NUI Interface Mappings

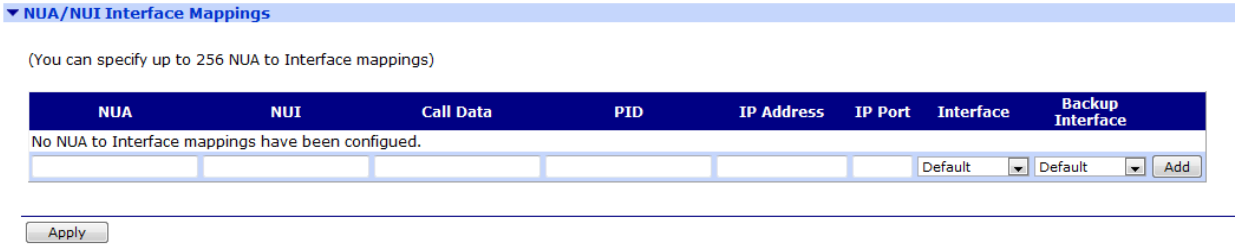
For PAD and TPAD instances, this table can be used to override the following:

- Interface
- Backup interface
- IP address
- TCP/UDP port number

Based upon data in the call request matching the following comparison fields:

- NUA called
- NUI called
- X.25 Call Data
- PID

All the comparison fields, NUA, NUI, Call Data and PID can use the wildcard matching characters “?” and “*”.



NUA
Network User Address

NUI
Network User Identifier

Call Data
X.25 Call Data

PID

Protocol Identifier

IP address
IP address

IP Port
IP port number

Interface
Primary interface

Backup Interface
Backup interface

Note that this table is duplicated in the ***Configuration - Network > Protocol Switch > NUA to Interface Mappings*** section as it can also be used by the Protocol Switch. Not all of the fields are visible in the Protocol Switch section as they do not all apply to the Protocol Switch.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
nuaip	N	nua	text	NUA
nuaip	N	nui	text	NUI
nuaip	N	cud	text	Call Data
nuaip	n	pid	text	PID
nuaip	n	IPaddr	IP address	IP Address
nuaip	n	ip_port	0 - 65535	IP Port
nuaip	n	swto	0 -15	Interface
nuaip	n	buswto	0 -15	Backup Interface

The interface and backup interface values are as follows:

Parameter Value	Interface Type
0	Default
1	LAPD
2	LAPB 0
3	LAPB 1
4	XOT
5	LAPD x (instance determined by NUA)
6	LAPB 0 PVC
7	LAPB 1 PVC
8	XOT PVC
9	TCP Stream
10	UDP Stream
12	LAPB 2

Parameter Value	Interface Type
13	LAPB 2 PVC
14	VXN
15	SSL

Calls Macros

Configuration – Network > Legacy Protocol > X.25> Calls Macros

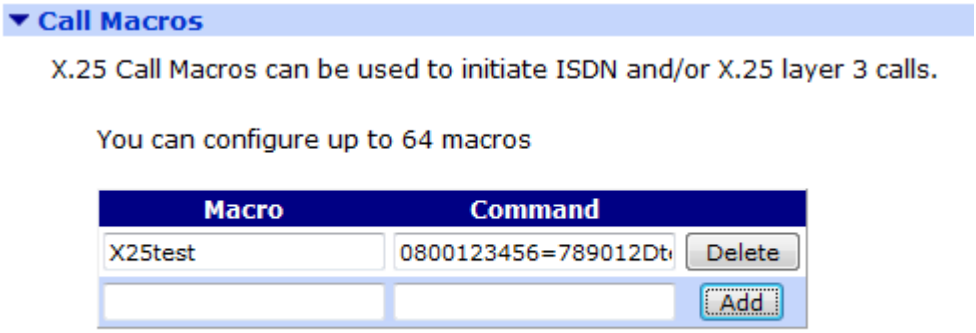
This page allows you to define up to 64 X.25 CALL "macros" that can be used to initiate ISDN and/or X.25 layer 3 calls. These simple English-like names are mapped to full command strings. For example, the call string:

0800123456=789012Dtest data

could be given the name "X25test" and then executed simply by entering:

CALL X25test

To create a macro, enter a name for the macro in the left column of the Call Macros table and in the right column enter the appropriate command string (excluding the ATD). Then click Add.



Macro
The name of the macro, this can be any text.

Command
The X.25 call command.

Related CLI Commands

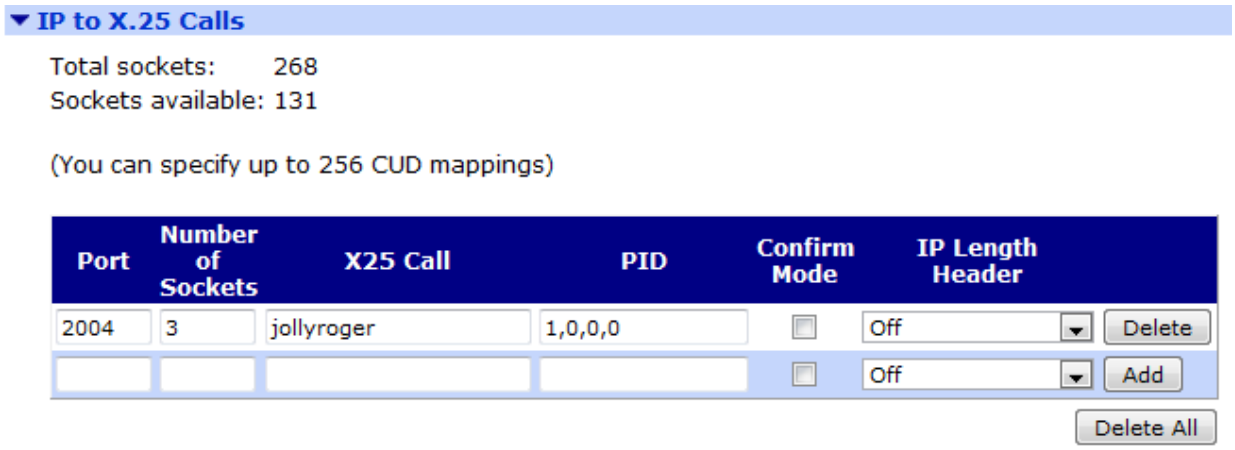
Entity	Instance	Parameter	Values	Equivalent Web Parameter
macro	n	name	text	Macro
macro	n	cmd	text	Command

IP to X.25 Calls

Configuration – Network > Legacy Protocol > X.25> IP to X.25 Calls

This page contains a table that allows you to enter a series of IP Port numbers and X.25 Call strings as shown below. It is used to configure the unit so that IP data can be switched over X.25. For example data that is received on a TCP connection can be answered by a PAD as if it is an X.25 call.

This table is duplicated in the ***Configuration - Network > Protocol Switch > IP Sockets to Protocol Switch*** section as it is also used by the protocol switch. It is included at this point in the web user interface as a convenience in case the table is being used in conjunction with PAD and not the protocol switch.



IP Port
The IP Port field is used to setup the port numbers for those IP ports that will "listen" for incoming connections that are to be switched over X.25 or other protocol. In the case of switching to X.25, when such a connection is made the unit will make an X.25 Call to the address specified in the X.25 Call field. Once this call has been connected, data from the port will be switched over the X.25 session.

Number of Sockets
The Number of Sockets field is used to select how many IP sockets should simultaneously listen for data on the specified port. The number of available IP sockets will depend on the model you are using and how many are already in use (see note below).

X25 Call
The X.25 call field may contain an X.25 NUA or NUI or one of the X.25 Call Macros defined on the ***Configuration - Advanced applications > X25 > Macros page***.

PID
The PID (Protocol Identifier), field specifies the PID to use when the unit switches an IP connection to X.25. The PID (protocol ID) field takes the format of four hexadecimal digits separated by commas, e.g. 1,0,0,0, at the start of the Call User Data field in the X.25 call.

Confirm Mode
When confirm mode is set to "On" then the incoming TCP socket will not be successfully connected until the corresponding outgoing call has been connected. The incoming TCP socket will trigger the corresponding outgoing call either to a local PAD instance or to whatever is configured. The effect of this mode is that the socket will fail if the outbound call fails and so may be useful in backup scenarios. In addition it will ensure that no data is sent into a "black hole". (When this setting is not enabled data that is sent on the inbound TCP connection before the outbound connection has been successful can be lost.)

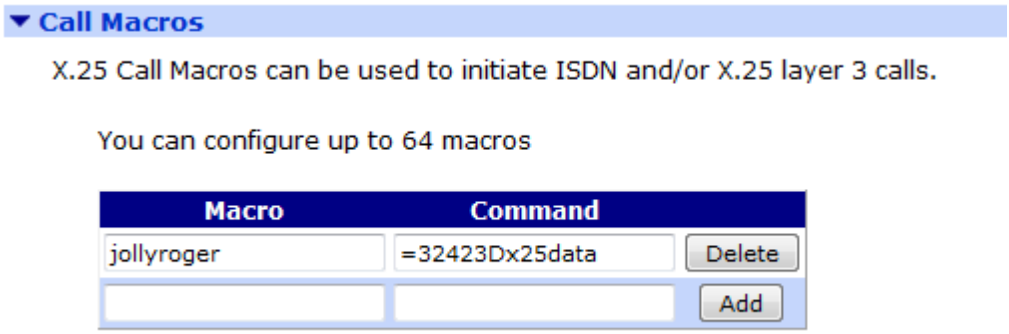
RFC 1086 Mode:

RFC 1086 specifies a mode of operation in which the IP socket answers and then with a simple protocol in the socket identifies the X.25 address and other X.25 call setup parameters to be used. Then when the X.25 call parameters have been identified the X.25 call is made and if successful then data is then switched between the X.25 call and the IP socket. The protocol will select whether incoming or outgoing support is required.

IP length header

When IP length header is "On", the IP length indicator field is inserted at the start of each packet. When set to "8583 Ascii 4 byte", the IP length header will conform to the ISO 8583 format.

In the example above, 3 IP sockets will "listen" for an incoming connection on IP Port 2004. Once connected they will each will make an X.25 Call to "jollyroger". The unit will recognise that "jollyroger" is a pre-defined macro (as illustrated below), and will translate it into an X.25 Call to address 32423 with the string "x25 data" included as data in the call. The outgoing X.25 call(s) will be made over whichever interface is specified by the Switch from XOT(TCP) to parameter on the ***Configuration - Network > Protocol Switch*** page.



Note:
At the top of the page the total number of sockets available and the number currently free is shown. Care should be take not to allocate too many of the free sockets unless you are confident that they are not required for other applications.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ipx25	n	ip_port	0 - 65535	IP Port
ipx25	n	nb_listens	0 – software dependant max	Number of Sockets
ipx25	n	x25call	NUA, NUI or X.25 macro name	X25 Call
ipx25	n	pid	hex numbers	PID
ipx25	n	cnf_mode	1 = enabled, 0 = disabled	Confirm Mode
ipx25	n	rfc1086_mode	1 = enabled, 0 = disabled	RFC 1086 Mode
ipx25	n	iphdr	0=Off 1=On	IP length header

Entity	Instance	Parameter	Values	Equivalent Web Parameter
			2=8583 Ascii 4 byte	

PADS n

Configuration – Network > Legacy Protocol > X.25> PADS n

PAD which stands for **P**acket **A**ssembler **D**issembler is used to interface between a character based serial connection and an X.25 synchronous packet switched network.

There are two main elements to the configuration procedure for accessing X.25 networks:

General and service related parameters

PAD parameters (X.3)

Each X.25 PAD configuration page also includes a sub-page detailing the X.3 PAD parameters. Collectively this set of values is known as a PAD profile. Your unit contains four pre-defined standard PAD profiles numbered 50, 51, 90 and 91. You may also create up to four custom PAD profiles numbered 1 to 4 for each PAD instance.

Use PAD over interface
This section is used to select whether the PAD instance will use ISDN B-channel X.25, ISDN D-channel X.25, TCP, UDP, VXN, SSL TCP or SSL XoT as the transport protocol. For ISDN D-channel operation, ensure that the “LAPD” option is selected. For ISDN B-channel operation or operation through a synchronous port, select “LAPB”. In the case of LAPB and LAPD it is also possible to specify an interface number. This parameter specifies which LAPB or LAPD instance to use for the relevant TPAD instance. Select “0” or “1” for LAPB or “0” or “1” for LAPD.

Use backup interface
This section is used to specify a backup interface that will be used automatically if the call to the primary interface fails. Note that the primary interface will be tried first for every new call attempt.

X.25 Settings

Default X.25 packet size
This parameter determines the default X.25 packet size. This may be set to “16”, “32”, “64”, “128”, “256”, “512” or “1024”, but the actual values permitted will normally be constrained by your service provider.

Answer incoming calls from NUA
This is the NUA that the unit responds to for incoming X.25 calls.

Only answer calls with CUG
The PAD will only answer calls with this Call User Group (CUG) specified.

Use X.25 Call Macro macroname to an ATD command
This parameter specifies the name of an X.25 call macro that is used when an ATD command is received by the unit. The ATD command is ignored, and a PAD CALL command using the macro replaces it. The purpose of this feature is to allow non-PAD terminals to use an X.25 PAD network connection. X.25 call macros are set up in the ***Configuration - Network > Legacy Protocols > X.25 > Call Macros*** web page, or by using the macro text command.

Use NUA
This NUA will be used as the calling NUA when an outgoing X.25 call is made.

LCN

The unit supports up to eight logical X.25 channels. In practice, the operational limit is determined by the particular service to which you subscribe (usually 4).

Each logical channel must be assigned a valid Logical Channel Number (LCN). The LCN parameter is the value of the first LCN that will be assigned for outgoing X.25 CALLs. The default is 1027.

For incoming calls, the unit accepts the LCN specified by the caller.

LCN Direction

This parameter determines whether the LCN used for outgoing X.25 calls is incremented or decremented from the starting value when multiple X.25 instances share one layer 2 (LAPB or LAPD), connection. The default is “Down” and LCNs are decremented, i.e. if the first CALL uses 1024, the next will use 1023, etc. Setting the parameter to “Up” will cause the LCN to be incremented from the start value.

NUI/NUA selection
If both an NUI and an NUA are included in the call string, this parameter allows the unit to filter one of these out of the X.25 call request. This can be extremely useful in backup scenarios. Consider the following example; the unit is configured to do online authorisations via the ISDN D channel and to fall back to B-channel (if the D-channel host did not respond for any reason). Using this parameter in conjunction with the backup equivalent, it is possible to configure the unit to use the supplied NUA to connect over D-channel and the supplied NUI to connect over B channel (for backup).

On the backup interface LCN
The LCN parameter is used to set the first LCN that will be used for the backup interface.

On the backup interface LCN Direction
This parameter determines whether the LCN used for the backup X.25 interface is incremented or decremented from the starting value when multiple X.25 instances share a single layer 2 connection.

On the backup interface NUI/NUA selection
If both an NUI and an NUA are included in the call string, this parameter allows the unit to filter one of these out of the X.25 call request.

Enable X.25 Restart Packets
It is normally possible to make X.25 CALLs immediately following the initial SABM-UA exchange. In some cases however, the X.25 network may require an X.25 Restart before it will accept X.25 CALLs. The correct mode to select depends upon the particular X.25 service to which you subscribe. The default value is “On”. This means that the unit WILL issue X.25 Restart packets. To prevent the unit from issuing Restart packets set this parameter to “Off”.

Restart delay
When the Restarts parameter is “On” the Restart Delay value determines the length of time in milliseconds that the unit will wait before issuing a Restart packet. The default value is 2000 giving a delay of 2 seconds.

IP Settings

Remote IP address
This field indicates the destination host that will answer the XOT, TCP, SSL, UDP call.

Remote IP Address when using the backup interface

This field indicates the destination host that will answer the XOT, TCP, SSL, UDP call if a connection via the primary interface has failed and the PAD is configured to backup to a secondary interface that is using an IP based protocol.

IP Stream port
This is the TCP or UDP port number to use for IP (but not XoT) connections.

IP length header
When set to “On”, and in IP Stream mode, the length of a data sequence is inserted before the data. For the receive direction it is assumed the length of the data is in the data stream. When set to “8583 Ascii 4 byte”, the IP length header will conform to the ISO 8583 format.

PAD Settings

PAD prompt
This parameter allows you to redefine the standard “PAD>” prompt. To change the prompt enter a new string of up to 15 characters into the text box.

PAD mode
The PAD Mode parameter can be set to “Normal” or “Prompt Always On”. In Prompt Always On mode, the ASY port attached to the PAD behaves as if it were permanently connected at layer 2, i.e. it always displays a “PAD>” prompt. AT commands may still be entered but the normal result codes are suppressed. To disable this mode set the parameter to “Normal”.

Use PAD Profile
The PAD profile # allows you to select the PAD profile to use for this PAD instance. There are four pre-defined profiles numbered “50”, “51”, “90” and “91”. In addition to the pre-defined profiles you can also create up to four user-defined profiles numbered “1”, “2”, “3” and “4”. To assign a particular profile to the PAD select the appropriate number from the list.

Strip Trailing Spaces
When this parameter is turned on any spaces received at the end of a sequence of data from the network will be removed before being relayed to the PAD port.

Enable Leased Line Mode
When this parameter is set to “On”, it causes the PAD to always attempt to be connected using the Auto macro setting as the call command.

Send ENQ on Connect
When this parameter is set to “On” the PAD will send an ENQ character on the ASY link when an outgoing call has been answered.

Enable STX / ETX Filtering
When this parameter is “On”, the PAD will ignore data that is not encapsulated between ASCII characters STX (Ctrl+B) and ETX (Ctrl+C). To disable this feature select the “Off” option.

Delay connect message n x 10 milliseconds
Delay the Connect message by the number of milliseconds specified. (Useful when working with equipment that previously connected to slower networks and is upset by the quicker “Connect” when used with modern networks.)

Delay data transfer after connection by n x 10 milliseconds
Delays the data delivered from the X.25 or other type of connection to the terminal upon initial connection.

Terminate the PAD call after x seconds if there has been no data transmission

This parameter specifies the length of time in seconds after which the PAD will terminate an X.25 call if there has been no data transmission.

Disconnect the layer 2 call if there is no layer 3 call in progress for x seconds
This parameter specifies the length of time in seconds after which the unit will disconnect a layer 2 link if there are no layer 3 calls in progress. For LAPB sessions this will also terminate the ISDN call.

Create an event when the following data is on the PAD
This parameter specifies a string, which if it appears in the received data causes a "Data Trigger" (47) event to be generated and recorded in the event log.

Create an event when there has been no activity on the PAD for x seconds
This specifies the time in seconds in which if there is no activity on the PAD an event in the event log will be posted. This can be used to trigger email exceptions.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
pad	n	l2iface	lapb, lapd, TCP, SSL	Use PAD over interface
pad	n	l2nb	0 – 255 (instance of LAPB or LAPD)	Use PAD over interface
pad	n	ip_stream	0 = off (for XoT), 1 = TCP, 2 = UDP	Use PAD over interface
pad	n	defpak	16,32,64,128,256,512 or 1024	Default X.25 packet size
pad	n	ansnua	text (valid NUA)	Answer incoming calls from NUA
pad	n	anscug	text (valid CUG)	Only answer calls with CUG
pad	n	amacro	text	Use X.25 Call Macro macroname to an ATD command
pad	n	cingnua	text (valid NUA)	Use NUA
pad	n	lcn	1 - 4095	LCN
pad	n	lcnup	1 = up, 0 = down	LCN Direction
pad	n	nuaimode	0 = NUI and NUA, 1 = NUA only, 2 = NUI only	NUI/NUA selection
pad	n	dorest	1 = enabled, 0 = disabled	Enable X.25 Restart Packets
pad	n	restdel	0 - 60000 (ms)	Restart delay
pad	n	IPaddr	text	Remote IP address
pad	n	buipaddr	text	Remote IP Address when using the backup interface
pad	n	ip_port	0 - 65535	IP Stream port

Entity	Instance	Parameter	Values	Equivalent Web Parameter
pad	n	iphdr	0=Off, 1=On, 2=8583 Ascii 4 byte	IP length header
pad	n	prompt	text	PAD prompt
pad	n	padmode	0 = Normal, 1 = Prompt Always On	PAD mode
pad	n	profile	1-4, 50, 51,90,91	Use PAD Profile
pad	n	strip_tspaces	1 = enabled, 0 = disabled	Strip Trailing Spaces
pad	n	llmode	1 = enabled, 0 = disabled	Enable Leased Line Mode
pad	n	enqcon	1 = enabled, 0 = disabled	Send ENQ on Connect
pad	n	stxmode	1 = enabled, 0 = disabled	Enable STX / ETX Filtering
pad	n	delconmsg	0 - 10	Delay connect message n x 10 millisecondss
pad	n	data_del	0 - 2147483647	Delay data transfer after connection by n x 10 milliseconds
pad	n	inacttim	0 - 1000	Terminate the PAD call after x seconds if there has been no data transmission
pad	n	nocalltim	0 - 60000	Disconnect the layer 2 call if there is no layer 3 call in progress for x seconds
pad	n	trig_str	text	Create an event when the following data is on the PAD
pad	n	inactevent	0 - 2147483647	Create an event when there has been no activity on the PAD for x seconds

Stopping and starting PADs

PAD instances can be stopped and started using the following CLI commands:

stoppads

gopads

The stoppads command stops all PAD instances from accepting and performing any PAD commands.

The gopads command resumes processing of PAD commands.

The stoppads and gopads commands can have the PAD number specified in the syntax to stop and start individual PAD instances.

For example:

To stop PAD 1 from processing PAD commands:

stoppads 1

and to re-enable PAD 1:

gopads 1

PADs 0-9 > PAD 0 >

Configuration – Network > Legacy Protocol > X.25> PADS 0 – 9> Pads 0

X3 Parameters

Configuration – Network > Legacy Protocol > X.25> PADS 0 – 9> Pads 0> X3 Parameters

Each PAD configuration page has an attached sub-page that allows you to edit the X.3 PAD parameters. These pages allow you to load one of the standard profiles or edit the individual parameters to suit your application requirements and save the resulting customised “user” profile to non-volatile memory.

Loading and Saving PAD Profiles

To create your own PAD profiles, edit the appropriate parameters and then select user profile 1, 2, 3 or 4 as required from the list and click the “Save Profile” button.

Each PAD profile page includes two list boxes that allow you to load and save PAD profiles. To load a particular profile, select the profile from the list and click the “Load Profile” button. The parameter table will be updated with the values from the selected profile.

1 PAD Recall Character
This parameter determines whether PAD recall is enabled. When this facility is enabled, typing the PAD recall character temporarily interrupts the call and returns you to the PAD> prompt where you may enter normal PAD commands as required. To resume the interrupted call, use the CALL command without a parameter.

The default PAD recall character is [Ctrl-P]. This may be changed to any ASCII value in the range 32-125 or disabled by setting it to 0.

When a call is in progress and you need to actually transmit the character that is currently defined as the PAD recall character, simply enter it twice. The first instance returns you to the PAD> prompt; the second resumes the call and transmits the character to the remote system.

Option	Description
0	Disabled
1	PAD recall character is CTRL-P (ASCII 16, DEL)
32 - 126	PAD recall character is user defined as specified

2 Echo
This parameter enables or disables local echo of data transmitted during a call. When echo is enabled, X.3 parameter 20 may be used to inhibit the echo of certain characters.

Option	Description
0	Echo off
1	Echo on

3 Data Forwarding Characters
This parameter defines which characters cause data to be assembled into a packet and forwarded to the network.

Option	Description
0	No data forwarding character
1	Alphanumeric characters (A-Z, a-z, 0-9)
2	CR
4	ESC, BEL, ENQ, ACK
8	DEL, CAN, DC2
16	EXT, EOT
32	HT, LF, VT, FF
64	Characters of decimal value less than 32

Combinations of the above sets of characters are possible by adding the respective values together. For example, to define CR, EXT and EOT as data forwarding characters, set this parameter to 18 (2 + 16).

If no forwarding characters are defined the Idle timer delay (parameter 4) should be set to a suitable value, typically 0.2 seconds.

4 Idle Timer Delay
This parameter defines a time-out period after which data received from the DTE is assembled into a packet and forwarded to the network. If the forwarding time-out is disabled, one or more characters should be selected as “data forwarding characters” using parameter 3.

Option	Description
0	No data forwarding time-out
1	Data forwarding time-out in 20ths of a second.

5 Ancillary Device Control
This parameter determines method of flow control used by the PAD to temporarily halt and restart the flow of data from the DTE during a call.

Option	Description
0	No flow control
1	XON/XOFF flow control
3	RTS/CTS flow control (not a standard X.3 parameter)

6 Suppression of PAD Service Signals
This parameter determines whether or not the “PAD>” prompt and/or Service/Command signals are issued to the DTE.

Option	Description
0	PAD prompt and signals disabled
1	PAD prompt disabled, signals enabled

Option	Description
4	PAD prompt enabled, signals disabled
5	PAD prompt enabled, signals disabled

7 Action on Break (from DTE)
This parameter determines the action taken by the PAD on receipt of a break signal from the DTE.

Option	Description
0	No action
1	Send an X.25 interrupt packet
2	Send an X.25 reset packet to the remote system
4	Send an X.29 indication of break
8	Escape to PAD command state
16	Set PAD parameter 8 to 1 to discard output

Multiple actions on receipt of break are possible by setting this parameter to the sum of the appropriate values for each action required.

For example, when parameter 7 is set to 21 (16 + 4 + 1), an X.25 interrupt packet is sent followed by an X.29 indication of break and then parameter 8 is set to 1.

You should NOT set this parameter to 16 because the remote system would receive no indication that a break had been issued and output to the DTE would therefore remain permanently discarded. If you need to use the discard output option, use it in conjunction with the X.29 break option so that on receipt of the X.29 break the remote system can re-enable output to your DTE using parameter 8.

8 Discard Output
This parameter determines whether data received during a call is passed to the DTE or discarded. It can only be directly set by the remote system and may be used in a variety of circumstances when the remote DTE is not able to handle a continuous flow of data at high speed.

Option	Description
0	Normal data delivery to DTE
1	Output to DTE discarded

9 Padding after CR
Slower terminal devices, such as printers, may require a delay after each Carriage Return before they can continue to process data. This parameter controls the number of pad characters (NUL - ASCII 0) that are sent after each CR to create such a delay.

Option	Description
0	No padding characters after CR
1 - 255	Number of padding characters (NUL) sent after CR

10 Line Folding

Controls the automatic generation of a [CR],[LF] sequence after a certain line width has been reached.

Option	Description
0	No line folding
1 - 255	Width of line before the PAD generates [CR],[LF]

11 Port Speed
This is a “read only” parameter, set automatically by the PAD and accessed by the remote system.

Option	Description
15	19,200 bps
14	9,600 bps
12	2,400 bps
3	2,400 bps

12 Flow Control of PAD (by DTE)
Determines the flow control setting of the PAD by the DTE in the on-line data state.

Option	Description
0	No flow control
1	XON/XOFF flow control
3	RTS/CTS flow control (not a standard X.3 parameter)

13 LF Insertion (after CR)
Controls the automatic generation of a Line Feed by the PAD.

Option	Description
0	No line feed insertion
1	Line Feeds inserted in data passed TO the DTE
2	Line Feeds inserted in data received FROM the DTE
4	Line Feeds inserted after CRs echoed to DTE

The line feed values can be added together to select Line Feed insertion to any desired combination.

14 LF Padding
Some terminal devices such as printers require a delay after each Line Feed before they can continue to process data. This parameter controls the number of padding characters (NUL - ASCII 0) that are sent after each [LF] to create such a delay.

Option	Description
0	No line feed padding.
1 - 255	Number of NUL characters inserted after LF

15 Editing

Enables (1) or disables (0) local editing of data input fields by the PAD before data is sent. The three basic editing functions provided are character delete, line delete and line re-display.

The editing characters are defined by parameters 16, 17 and 18. In addition, parameter 19 determines which messages are issued to the DTE during editing.

When editing is enabled, the idle timer delay (parameter 4) is disabled and parameter 3 must be used to select the desired data forwarding condition.

16 Character Delete Character
This parameter defines the edit mode delete character (ASCII 0-127). The default is backspace (ASCII 08).

17 Line Delete Character
This parameter defines the edit mode line buffer delete character (ASCII 0-127). The default is CTRL-X (ASCII 24).

18 Line Redisplay Character
Specifies the character that re-displays the current input field when in editing mode (ASCII 0-127). The default is CTRL-R (ASCII 18).

19 Editing PAD Service Signals
Specifies the type of service signal sent to the DTE when editing input fields.

Option	Description
0	No editing PAD service signals
1	PAD editing service signals for printers
2	PAD editing service signals for terminals

20 Echo Mask
This parameter defines characters that are NOT echoed when echo mode has been enabled using parameter 2.

Option	Description
0	No echo mask (all characters are echoed)
1	CR
2	LF
4	VT, HT or FF
8	BEL, BS
16	ESC,ENQ
32	ACK,NAK,STX,SOH,EOT,ETB,ETX
64	No echo of characters set by parameters 16, 17 & 18
128	No echo of characters set by parameters 16, 17 & 18

Combinations of the above sets of characters are possible by adding the respective values together.

21 Parity Treatment
This parameter determines whether parity generation/checking is used.

Option	Description
0	No parity generation or checking
1	Parity checking on
2	Parity generation on
3	Parity checking and generation on

22 Page Wait

This parameter determines how many line feeds are sent to the terminal before output is halted on a page wait condition. In other words, it defines the page length for paged mode output. A page wait condition is cleared when the PAD receives a character from the terminal.

Option	Description
0	Page wait feature disabled
1	Number of line feeds sent before halting output

Related CLI Commands

The X.3 PAD parameters can be edited from the command line using the **set** command described under the X.28 Commands section.

X.25 PVCs

Configuration – Network > Legacy Protocol > X.25> X.25 PVCs

A Permanent Virtual Circuit (PVC) provides the X.25 equivalent of a leased line service. With a PVC there is no call setup or disconnect process; you can just start sending and receiving X.25 data on a specified LCN. For each X.25 service connection you may setup up multiple PVCs each of which uses a different LCN (or a mixture of PVCs and SVCs). Digi routers support up to four PVCs numbered 0-3.

X.25 PVC n

Configuration – Network > Legacy Protocol > X.25> X.25 PVCs> X.25 PVC n

Enable this PVC
Enables or disables the PVC.

LCN
This is the LCN value to be used for this PVC. In the case of an XOT PVC, this parameter defines the Responder LCN field in the PVC setup packet (though an LCN of 1 is always used in the XOT PVC connection). So for an XOT PVC this field should contain the remote connections LCN.

PVC Mode
This parameter defines the lower layer interface to be used for the PVC and can be set to "LAPB", "LAPD" or "TCP" (for XOT mode).

Connect this PVC to PAD x
This parameter defines what type of upper layer interface is connected to this PVC and can be set to "PAD" (for an X.25 PAD), "TPAD" (for a TPAD instance) or "XSW" (for X.25 switching). Note that if set to "XSW" (for the X.25 switch) then the X.25 switch will need to also be configured regarding the interfaces to switch this PVC to/from. For example, if this is an incoming XOT PVC we are configuring then the Switch from XOT PVC parameter needs to be set to the desired destination interface.

Use packet size
This parameter defines the packet size to be used for the PVC. Select the appropriate value from the drop down list.

Use window size
This parameter defines the layer 3 window size to be used for the PVC. Select the appropriate value from the drop down list.

Remote IP address
This is the IP address to be used for outgoing XOT calls.

Use the source IP address from interface x,y
This parameter defines which Ethernet or PPP interface to use for the source IP address.

Initiator interface
This parameter may be set to the name of the interface from which the PVC was initiated, e.g. Serial 1. The initiator and responder strings are used to identify the circuit when PVCs are being set up. They must match the names in the remote unit that terminates the XOT PVC connection. If the unit terminating the PVC XOT connection is not another Digi unit then you need to refer to the documentation or the configuration files of the other unit to determine the names of the interfaces.

Responder interface

This parameter may be set to the name of the interface to which a PVC initiator is connected, e.g. Serial 2.

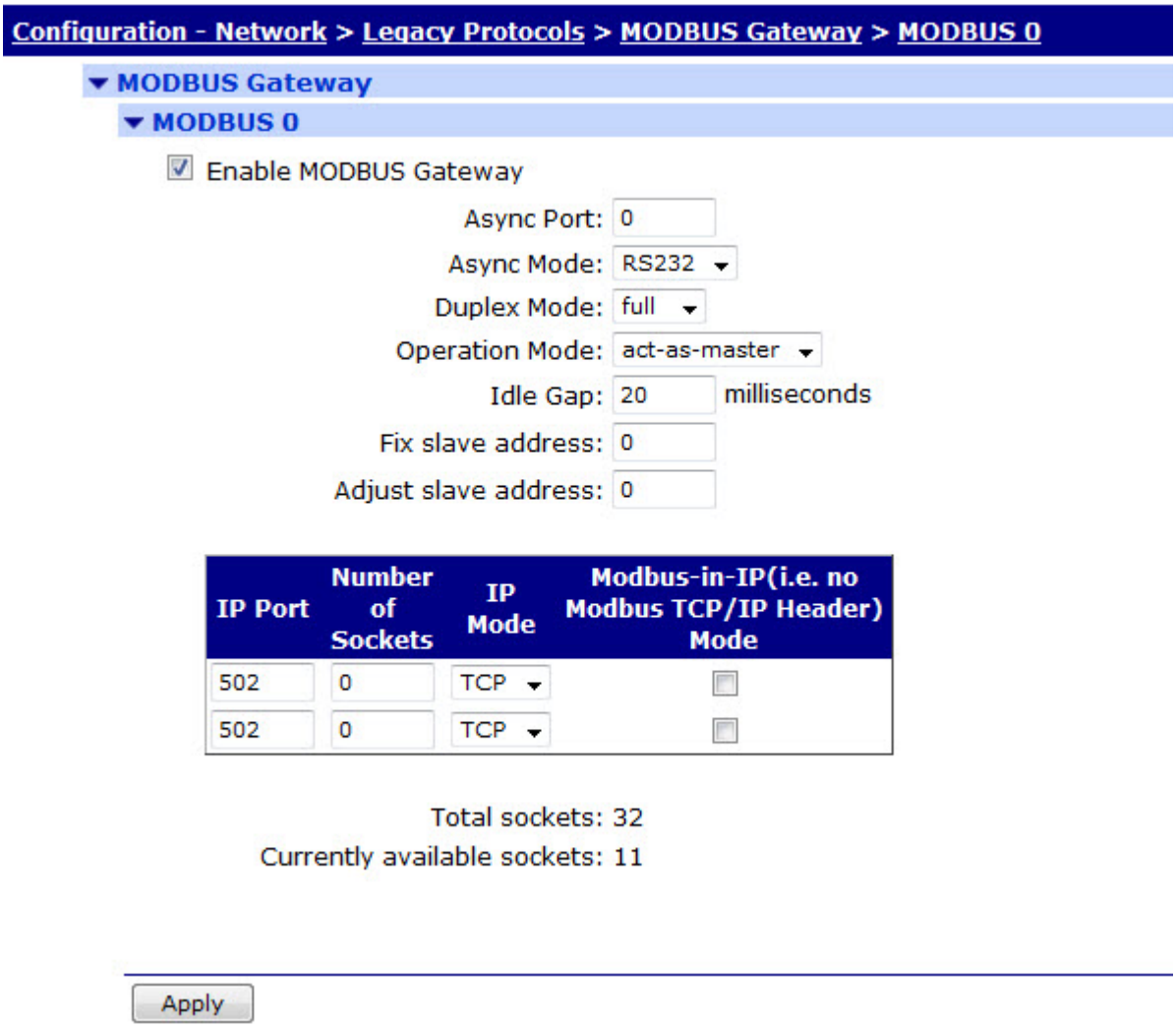
Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
pvc	n	l2iface	Blank or lapb, lapd, tcp	Enable this PVC
pvc	n	lcn	0 - 4096	LCN
pvc	n	uliface	pad, tpad, xsw	Connect this PVC to PAD x
pvc	n	psize	0=default 4=16 5=32 6=64 7=128 8=256 9=512 10=1024	Use packet size
pvc	n	window	1 - 7	Use window size
pvc	n	ipaddr	IP address	Remote IP address
pvc	n	srcipent	auto, eth, ppp	Use the source IP address from interface x,y
pvc	n	srcipadd	0 - 255	Use the source IP address from interface x,y
pvc	n	iniface	text	Initiator interface
pvc	n	respiface	text	Responder interface

MODBUS Gateway

Configuration – Network > Legacy Protocol > MODBUS Gateway

Digi TransPort routers support conversion from MODBUS serial to MODBUS TCP.



When converting from MODBUS serial to MODBUS TCP over a WAN link it is necessary to have intelligence in the gateway\router to minimise the effect of the higher latency.

Digi TransPort supports being a MODBUS server only. Clients (e.g. remote PCs) can send overlapping requests and the Digi TransPort will create a queue of info requests and deal with them appropriately sending them out over the serial port and relaying the responses back. Overlapping polls from multiple clients are supported.

Enable MODBUS Gateway
Enables or disables MODBUS gateway instance.

Async Port
Configure the local serial port number (asynchronous port) for the MODBUS serial interface.

Async Mode
Configures the serial driver for RS232 or RS485 on supported hardware.

Duplex Mode
Sets the duplex mode to half or full. Full would be for 4-wire installations otherwise half is required.

Operation mode
This parameter sets the operation mode to master or slave.

Idle Gap
When receiving an modbus response from a station when this idle gap (pause with no reception of characters) is detected the message (currently received from the station) is at that staged forwarded on as the complete response.

Fix slave address
The address of the slave is fixed at this value. An address conversion will take place if a message that does not contain this address is received from the TCP master. If not used the TCP master must use the correct slave address.

Adjust slave address
The address of the slave is adjusted by this value. If left to zero then the slave address is not adjusted at all.

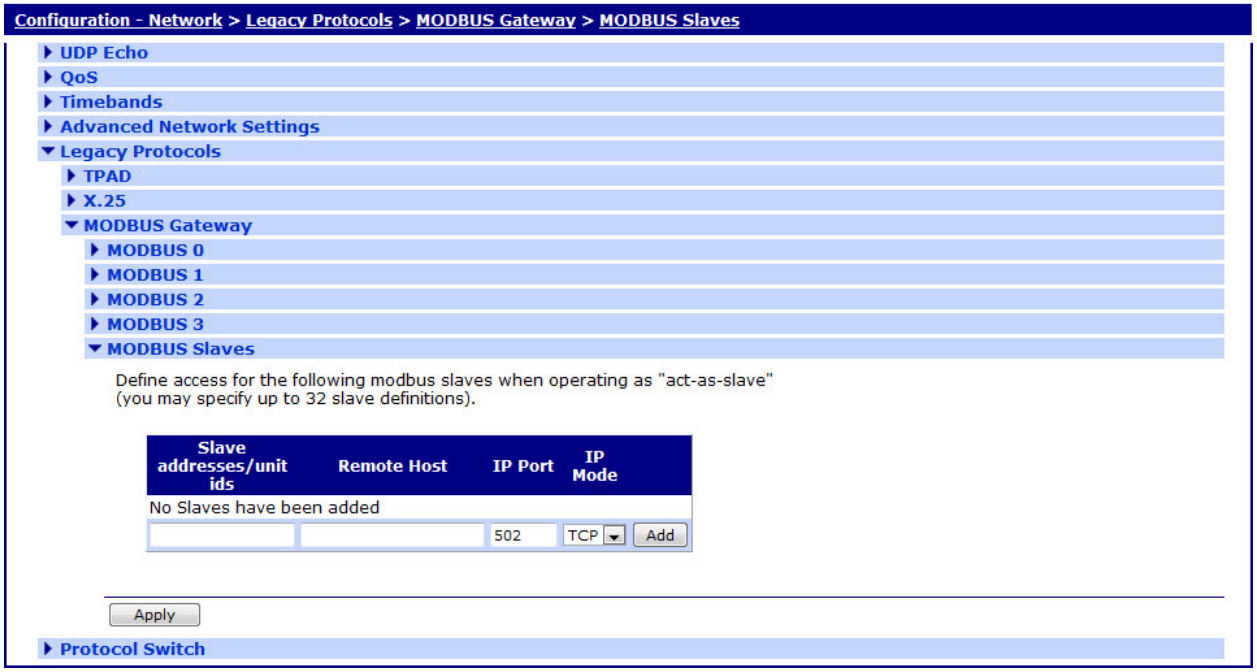
Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
modbus	n	enabled	1 = enabled, 0 = disabled	Enable MODBUS Gateway
modbus	n	asy_add	0 - 255	Async Port
modbus	n	op_mode	Master/Slave	Operation mode
modbus	n	async_mode	RS322 or RS422	Async Mode
modbus	n	duplex	0 = full, 1 = half	Duplex Mode
modbus	n	idle_gap	0 - 2147483647	Idle Gap
modbus	n	fix_slave_address	0 - 255	Fix slave address
modbus	n	adj_slave_address	0 - 255	Adjust slave address
modbus	n	ipport0	0 - 65535	IP Port (row 1)
modbus	n	nbsocks0	0 - “currently available”	Number of sockets (row 1)
modbus	n	ipmode0	0 = TCP, 1 = UDP	IP Mode (row 1)
modbus	n	rawmode0	1 = enabled, 0 = disabled	Raw Mode (row 1)
modbus	n	Ipport1	0 - 65535	IP Port (row 2)
modbus	n	nbsocks1	0 - “currently available”	Number of sockets (row 2)
modbus	n	ipmode1	0 = TCP, 1 = UDP	IP Mode (row 2)

Entity	Instance	Parameter	Values	Equivalent Web Parameter
modbus	n	rawmode1	1 = enabled, 0 = disabled	Raw Mode (row 2)
modbus	n	bcasts_on	OFF, ON	Broadcast support.

MODBUS Slaves

Configuration – Network > Legacy Protocol > MODBUS Gateway> MODBUS Slaves



This page defines access for the following MODBUS slaves when operating as "act-as-slave". Up to 32 slave definitions may be defined.

Slave addresses/unit ids
This field specifies the address of the slave unit.

Remote Host
The value in this text box specifies the IP address of the remote host, i.e. the slave unit.

IP Port
This is the IP port number. The default port is 502.

IP Mode
Select the IP mode using this drop down list. The default mode is TCP.

Add
Click on the add button to add the slave.

Protocol Switch

Configuration – Network > Protocol Switch

The Protocol Switch software available on some models provides X.25 call switching between the various protocols and interfaces that may be available including:

Interface / Protocol	Description
Off/None	Data will not be switched from / backed-up to this protocol
LAPD	Data will be switched from / backed-up to LAPD using the X.25 service.
LAPD X	As above but the actual LAPD instance used will be determined by the NUA.
LAPB 0	Data will be switched from / backed-up to LAPB 0.
LAPB 1	Data will be switched from / backed-up to LAPB 1.
LAPB 2	Data will be switched from / backed-up to LAPB 2.
LAPB 0 PVC	Data will be switched from / backed-up to an X.25 PVC on LAPB 0.
LAPB 1 PVC	Data will be switched from / backed-up to an X.25 PVC on LAPB 1.
LAPB 2 PVC	Data will be switched from / backed-up to an X.25 PVC on LAPB 2.
XoT	Data will be switched from / backed-up to an XOT (X.25 over TCP/IP) connection.
XoT PVC	Data will be switched from / backed-up to an XOT PVC connection.
TCP stream	Data will be switched from / backed-up to a TCP socket. The socket's IP address will be determined from the IP stream port setting.
UDP stream	This is similar to the TCP stream setting but instead of switching onto a TCP socket, data is switched onto a UDP socket. In the case of switching from X.25. the effect is that a UDP frame will be sent for each packet of X.25 data being switched.
VXN	Data will be switched / backed-up to Datawire's VXN protocol
SSL	Data will be switched / backed-up to SSL
DialServ	Data will be switched backed-up to an analogue modem via the built in DiaslServ daughter card.

When this optional feature is included, the unit may be configured to pass X.25 calls or data received in a TCP connection to another protocol or interface.

In addition, it is possible to specify a backup protocol or interface so that if an outgoing call on one interface fails, then the backup interface is automatically tried. LAPB can be used to switch to either ISDN or X.25 over serial depending on the configuration of the LAPB instance chosen.

The logic used in the switching software is outlined in the flowchart below. The following notes provide a more in-depth explanation of the actions taken in each of the numbered boxes.

The unit will first look up the Called NUA/NUI in the Configuration - Network > Protocol Switch > NUA to Interface Mappings mapping table to determine the IP address to use in the event that the call ends up being switched to a TCP or XOT interface. If a match is found on the Called NUA/NUI the unit assigns the matching IP address from the table to the call. If IP address mapping table does not contain an entry for the Called NUA/NUI and the call is eventually switched to a TCP or XOT channel then the default IP address (IP Stream or XOT Remote IP Address) is used.

The unit then determines from the source interface of the incoming call which interface type it should be switched to (from the Switch from parameters on the Protocol Switch page). For example, if the call arrived via a LAPB 0 interface and the Switch from LAPB 0 to parameter was set to LAPD, then the outgoing interface would LAPD.

If the outgoing interface is LAPD the unit changes the Calling NUA field of the incoming call to the D-Channel NUA value (as defined on the Protocol Switch page). If the outgoing interface is NOT LAPD processing proceeds as at step 6.

The unit then searches the Configuration - Network > Protocol Switch > NUA Mappings table to see if there are any matches for the Called or Calling NUA values on the specified interface. In cases where there Interface Description Off/None Data will not be switched from / backed-up from this protocol is a match, the NUA In value is substituted by the NUA out value, i.e. the mapping is applied individually to both the Calling NUA and Called NUA for the packet.

The unit then checks the leading characters of the Calling NUA to see if there is a match with the Call Prefix parameter. If there is a match then the prefix digits are removed before the outgoing X.25 call is made. Otherwise the call is made anyway and the switching process is complete for this call.

If after step 3, the unit has determined that the outgoing interface is not LAPD, it checks if the outgoing interface is LAPB. If it is, it then checks to see if the Called NUA field in the call packet matches the LAPB 0 NUA parameter and if it does, selects LAPB 0 as the outgoing interface. If the Called NUA field does not match LAPB 0 NUA, it checks for a match with LAPB 1 NUA and if there is a match, sets the outgoing interface to LAPB 1.

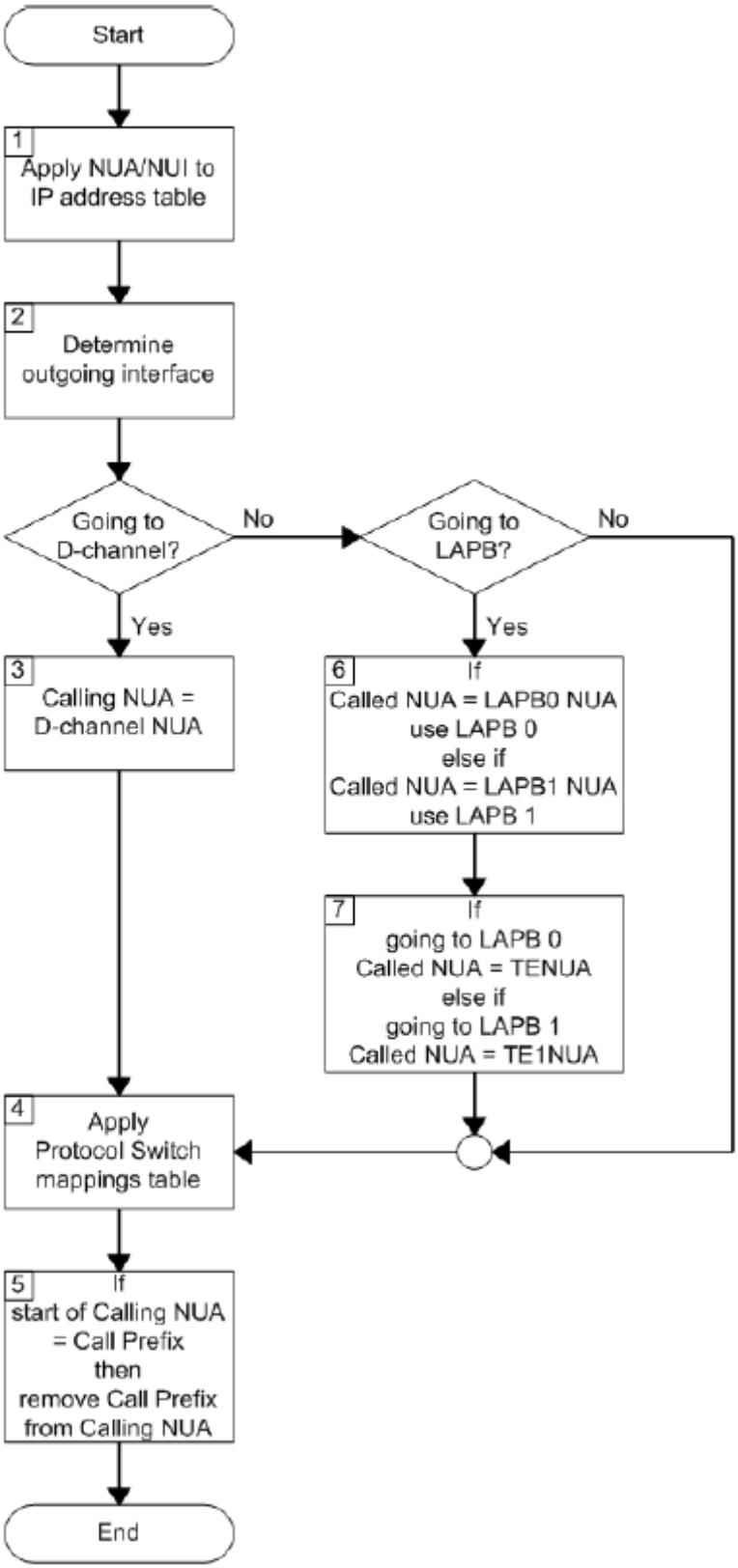
If the Called NUA field in the calling packet matches neither the LAPB 0 NUA or LAPB 1 NUA parameters then the outgoing interface is set to the interface specified by the relevant Switch from parameter.

If the call is being switched over LAPB 0 the unit then sets the Called NUA to the TE NUA (LAPB 0) value. If the call is being switched over LAPB 1 the unit then sets the Called NUA to the TE NUA (LAPB 1) value.

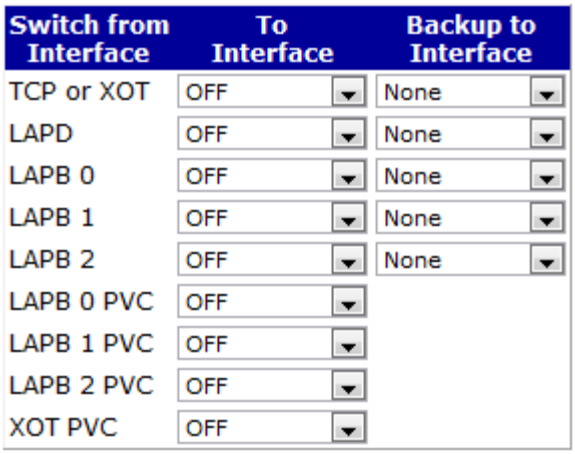
The ***Configuration – Network > Protocol Switch*** menu has the following sub-menu options:

- CUD Mappings

- IP Sockets to Protocol Switch
- NUA to Interface Mappings
- NUA Mappings


Start
1
Apply NUA/NUI to IP address table
2
Determine outgoing interface
Going to D-channel?
No
Going to LAPB?
No
Yes
Yes
3
Calling NUA = D-channel NUA
6
If
Called NUA = LAPB0 NUA
use LAPB 0
else if
Called NUA = LAPB1 NUA
use LAPB 1
7
If
going to LAPB 0
Called NUA = TENUA
else if
going to LAPB 1
Called NUA = TE1NUA
4
Apply Protocol Switch mappings table
5
If
start of Calling NUA = Call Prefix
then
remove Call Prefix from Calling NUA
End

Parameters



TCP or XoT
This parameter controls the switching of incoming X.25 calls received via TCP or XOT. Select the interface to which data should be switched from the drop down list, or select “Off” and the protocol switch will not respond to any incoming XOT or TCP connections.

LAPD
This parameter controls the switching of incoming X.25 calls received via ISDN LAPD. Select the interface to which data should be switched from the drop down list, or select “Off” and the protocol switch will not respond to any incoming LAPD calls.

LAPB X
This parameter controls the switching of incoming X.25 calls received via LAPB X. Select the interface to which data should be switched from the drop down list, or select “Off” and the protocol switch will not respond to any incoming LAPB X calls.

LAPB X PVC
This parameter controls the switching of incoming X.25 calls received via an LAPB X PVC. Select the interface to which data should be switched from the drop down list, or select “Off” and the protocol switch will not respond to any incoming PVC calls on LAPB X.

XOT PVC
This parameter controls the switching of incoming X.25 calls received via an XOT PVC. Select the interface to which data should be switched from the drop down list, or select “Off” and the protocol switch will not respond to any incoming XOT PVC calls.

TCP XOT backup to interface
If any of the Switch from parameters has been set to XOT, and XOT is unavailable, this parameter may be used to specify an alternative interface to switch the X.25 call to. Any of the other interfaces may be chosen, or “None”. If “None” is chosen, then no backup call will be attempted.

LAPD backup to interface
If any of the Switch from parameters has been set to LAPD, and LAPD is unavailable, this parameter may be used to specify an alternative interface to switch the X.25 call to. Any of the other interfaces may be chosen, or “None”. If “None” is chosen, then no backup call will be attempted.

LAPB X backup to interface
If any of the Switch from parameters has been set to LAPB X, and LAPB X is unavailable, this parameter may be used to specify an alternative interface to switch the X.25 call to. Any of the other interfaces may be chosen, or “None”. If “None” is chosen, then no backup call will be attempted.

VXN backup to interface
If any of the Switch from parameters has been set to VXN, and VXN is unavailable, this parameter may be used to specify an alternative interface to switch the X.25 call to. Any of the other interfaces may be chosen, or “None”. If “None” is chosen, then no backup call will be attempted.

LAPD Parameters

Calling Prefix
This parameter specifies the call prefix to inserted in front of the NUA in calls being switched to LAPD. For example, if the called NUA in the call being received by the LAPB 0 interface is 56565 and the call prefix is 0242 then the call placed on the LAPD interface is to NUA 024256565. Also, for calls in the reverse direction, if the prefix in the calling NUA matches this parameter then it is removed from the calling NUA field.

D-Channel LCN
This is the value of the first LCN that will be assigned for outgoing X25 calls on LAPD.D-Channel LCN Direction

Max VCs: Unlimited
This parameter sets the maximum number of Virtual Circuits (VCs) to be used on an LAPD interface. When the maximum has been reached, then the backup call will take place immediately (or the call will clear if there is no backup call). If this parameter is set to “0”, there is no limit.

Default Packet Size
This is the default packet size for X.25 calls being switched onto LAPD. The default packet size is 128, other possible values are 256, 512 or 1024 bytes.

Default Window Size
This is the default window size for calls being switched onto LAPD. The default window size is 2, the valid range is 1 to 7.

LAPB Parameters

LCN
This is the value of the first LCN that will be assigned for outgoing X25 calls on LAPB.

LCN direction: Up Down
This parameter determines whether the LCN used for outgoing X.25 calls on LAPB is incremented or decremented from the starting value.

Max VCs: Unlimited
This parameter sets the maximum number of Virtual Circuits (VCs) to be used on an LAPB interface. When the maximum has been reached, then the backup call will take place immediately (or the call will clear if there is no backup call). If this parameter is set to “0”, there is no limit.

B-Channel Number:
This parameter specifies an ISDN number to be used for calls being switched in the direction of LAPB 0 or LAPB 1.

Enable ENQ Char:
When this parameter is set to “On”, when an incoming call on LAPB is switched and the unit connects to it, the X.25 switch sends a data packet on the LAPB X.25 SVC containing the ENQ character.

LAPB 0 Default Packet Size: 128 256 512 1024
This is the default packet size for calls being switched onto LAPB 0. The default packet size is 128, other possible values are 256, 512 or 1024 bytes.

LAPB 0 Default Window Size: 2 1 3 4 5 6 7
This is the default window size for calls being switched onto LAPB 0. The default window size is 2, the valid range is 1 to 7.

LAPB 1 Default Packet Size: 128 256 512 1024
This is the default packet size for calls being switched onto LAPB 1. The default packet size is 128, other possible values are 256, 512 or 1024 bytes.

LAPB 1 Default Window Size: 2 1 3 4 5 6 7
This is the default window size for calls being switched onto LAPB 1. The default window size is 2, the valid range is 1 to 7.

LAPB 2 Default Packet Size: 128 256 512 1024
This is the default packet size for calls being switched onto LAPB 2. The default packet size is 128, other possible values are 256, 512 or 1024 bytes.

LAPB 2 Default Window Size: 2 1 3 4 5 6 7
This is the default window size for calls being switched onto LAPB 2. The default window size is 2, the valid range is 1 to 7.

IP Stream / XOT Parameters

IP Stream or XOT Remote IP Address:
For calls being switched in the direction of XOT, this parameter specifies the destination IP address to be used for the outgoing XOT call. This is also used as the destination IP address in the IP/UDP stream modes.

IP Stream or XOT Backup IP Address:
If the Switch from XOT to parameter is set to “XOT”, this is the IP address that the XOT call will be switched to, in the event the original XOT IP address is unavailable.

IP Stream Port:
This parameter determines the IP port number used when IP stream or UDP stream are selected as the parameter for any of the Switch from or Backup from parameters.

Note:
The XOT remote IP address and IP stream port parameters will be overridden by the values in the NUA/NUI to IP addresses table if the call matches any entry in that table.

IP Length Header: Off On 8583 Ascii 4 byte On(inclusive)
When IP length header is “On”, a length indicator field is inserted at the start of each packet. When set to “8583 Ascii 4 byte”, the IP length header will conform to the ISO 8583 format.

Source IP address interface: Auto Ethernet PPP
The default value for this parameter is “Auto”, which means that the source IP address of an outgoing XOT connection on an un-NATed W-WAN link is the address of the PPP interface assigned to W-WAN. This is because the XOT connection is initiated (automatically) within the router and so does not originate from the local subnet (LAN segment to which the unit is attached via the Ethernet interface).

However, this means that if you are routing traffic from the local subnet across a VPN tunnel you would have to set up two Eroutes; one to match the local subnet address and one to match the XOT source address (i.e. the address of the PPP interface associated with to the wireless network).
By setting this parameter to “Ethernet” the unit will use the IP address of the Ethernet port instead of that of the PPP interface so that you need only set up on Eroute.

X.25 Parameters

Don't switch facilities:
If this parameter is set to “Off”, the packet size and window size are only switched if they need to, i.e. they specify a value different from what is currently being negotiated. If this parameter is set to “On”, the facilities shall not be switched.

Don't strip facilities:
When set to “On” this parameter stops the X.25 switch from stripping packet size and window size facilities as it switches an X.25 call. When set to “Off”, the X.25 switch will strip facilities if the requested facilities match the defined defaults for that interface.

L2 Deactivation Clear Cause:
When one side of a switch call fails because layer 2 drops, the other side is usually cleared with a clear cause 9 “out of order”. This parameter allows you to set this code to any value.

X25 Version: 84 88
This parameter allows you to switch between X.25 version 88, and X.25 version 84, in which clear causes are always “0” when issued if the unit is the DTE.

Interpret no facilities on Call Accept as P7W2:
When this parameter is set to “On”, the X.25 switch will interpret any call accept packets that do not include the window size (’W’) or packet size (’P’) as if the call accept has ’P7W2’ (i.e. a packet size of 128 bytes and a windows size of 2).

Notes on PAD Answering
Because the other interfaces can operate as normal, even when the switch is operating, special care needs to be taken with regard to answering NUAs programmed on active PADs. For example when a call is being received on a LAPD or LAPB interface, a PAD instance (or remote configuration session) is capable of answering and terminating the call in preference to the call being switched. This means that the PADs “Answering NUA” parameters should be left blank to ensure that the unit’s PADs are not answering calls that need to be switched. If you do want a PAD instance to answer a call then program the “Answering NUA” field with as many digits as you can to ensure it only answers calls destined for that PAD. The same precautions apply to the **Allow CLI access from X.25 address** parameter on the ***Configuration - System > General*** page.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
X25sw	0	swfrlapb0	0,1,3- 10,12-15 (see below)	Switch from LAPB 0 to
X25sw	0	swfrlapb0pvc	0-5,7-10,12-15 (see below)	Switch from LAPB 0 PVC to
X25sw	0	swfrlapb1	0-2,4-10,12-15 (see below)	Switch from LAPB 1 to
X25sw	0	swfrlapb1pvc	0-6,8-10,12-15 (see below)	Switch from LAPB 1 PVC to

Entity	Instance	Parameter	Values	Equivalent Web Parameter
X25sw	0	swfrlapb2	0-10,13-15 (see below)	Switch from LAPB 2 to
X25sw	0	swfrlapb2pvc	0-10,12, 14, 15 (see below)	Switch from LAPB 2 PVC to
X25sw	0	swfrlapd	0, 2-10,12-15 (see below)	Switch from LAPD to
X25sw	0	swfrxot	0-3,5-10,12-15 (see below)	Switch from XOT (TCP) to
X25sw	0	swfrxotpvc	0-7,9,10,12-15 (see below)	Switch from XOT PVC to
X25sw	0	callprefix	<NUA>	Calling Prefix
X25sw	0	dlcn	0-65535	D-Channel LCN
X25sw	0	dlcnup	off, on Off = Down On = Up	D-Channel LCN Direction
X25sw	0	dmaxvc	0-65535	Max VCs
X25sw	0	lapb0ppar	7,8,9,10 7=128 8=256 9=512 10=1024	Default Packet Size
X25sw	0	lapb0wpar	1-7	Default Window Size
X25sw	0	blcn	0-65535	LCN
X25sw	0	blcnup	off, on Off = Down On = Up	LCN direction
X25sw	0	bmaxvc	0-65535	Max VCs
X25sw	0	bnumber	ISDN number	B-Channel Number
X25sw	0	benqcon	off, on	Enable ENQ Char
X25sw	0	lapdppar	7,8,9,10 7=128 8=256 9=512 10=1024	LAPB 0 Default Packet Size
X25sw	0	lapdwpar	1-7	LAPB 0 Default Window Size
X25sw	0	lapb1ppar	7,8,9,10 7=128 8=256 9=512 10=1024	LAPB 1 Default Packet Size
X25sw	0	lapb1wpar	1-7	LAPB 1 Default Window Size

Entity	Instance	Parameter	Values	Equivalent Web Parameter
X25sw	0	lapb2ppar	7,8,9,10 7=128 8=256 9=512 10=1024	LAPB 2 Default Packet Size
X25sw	0	lapb2wpar	1-7	LAPB 2 Default Window Size
X25sw	0	ipaddr	IP address	IP Stream or XOT Remote IP Address
X25sw	0	buipaddr	IP address	IP Stream or XOT Backup IP Address
X25sw	0	ip_port	0-65535	IP Stream Port
X25sw	0	iphdr	0,1,2 0=Off 1=On 2=8583 Ascii 4 byte	IP Length Header
X25sw	0	srcipadd	Interface number 0-65535	Source IP address interface
X25sw	0	srcipent	<blank>, PPP, ETH	Source IP address interface
X25sw	0	noswfac	off, on	Don't switch facilities
X25sw	0	nostripfac	off, on	Don't strip facilities
X25sw	0	l2deactcc	0-65535	L2 Deactivation Clear Cause
X25sw	0	x25ver84	off, on Off=88 On=84	X25 Version
X25sw	0	accdefp7w2	off, on	Interpret no facilities on Call Accept as P7W2

Interfaces are coded as follows:

Parameter value	Interface type
0	None
1	LAPD
2	LAPB 0
3	LAPB 1
4	XOT
5	LAPD X (actual instance is determined by NUA)
6	LAPB 0 PVC
7	LAPB 1 PVC
8	XOT PVC
9	TCP stream

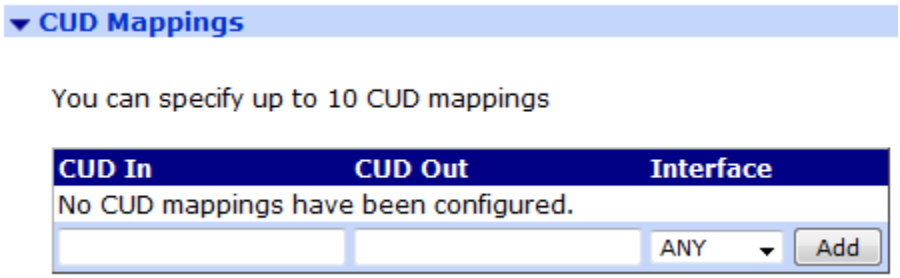
Parameter value	Interface type
10	UDP stream
12	LAPB 2
13	LAPB 2 PVC
14	VXN
15	SSL

CUD Mappings

Configuration - Network > Protocol Switch > CUD Mappings

Protocol Switch CUD mappings allow you to map an incoming call's CUD (call user data) from one value to another. The PID (protocol identifier) portion of the CUD (if present) is maintained from input to output and is not involved in the comparison.

The ***Configuration - Network > Protocol Switch > CUD Mappings*** web page displays a table with four columns in which you can specify the CUD In values, corresponding CUD Out values and to which interfaces the mappings should be applied. The "interface" field defines which output interfaces this mapping applies to. Wildcard characters are allowed, and In each case the interface type to which the mapping applies can be selected from "ANY", "LAPD", "LAPB0", "LAPB1" "LAPB2" or "XOT".



Related CLI Commands

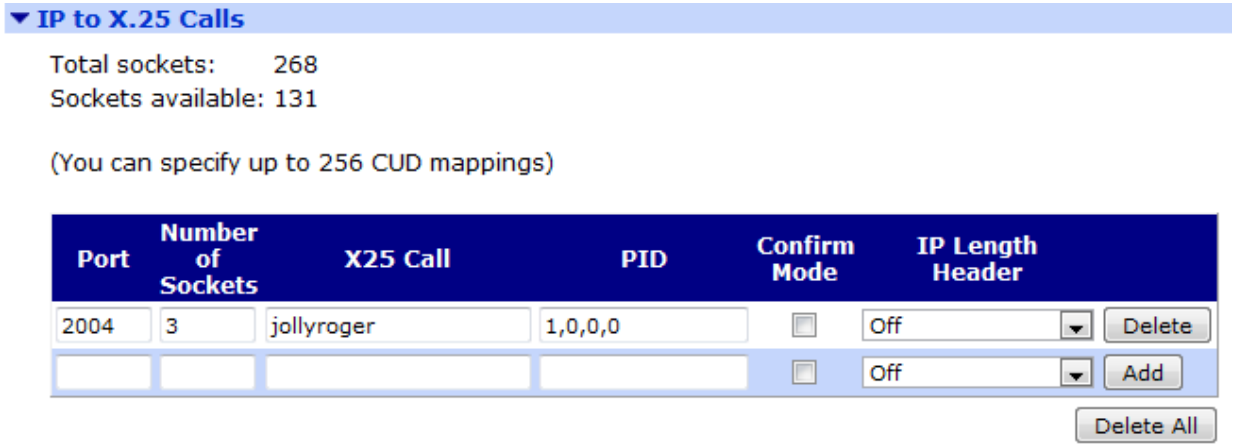
Entity	Instance	Parameter	Values	Equivalent Web Parameter
cudmap	0-9	cudfrom	0-65536	CUD In
cudmap	0-9	cudto	0-65536	CUD Out
cudmap	0-9	Interface	0,1,2,3,4,12 0=Any 1=LAPD 2=LAPB 0 3=LAPB 1 4=XOT 12=LAPB 2	Interface

IP Sockets to Protocol Switch

Configuration - Network > Protocol Switch > IP Sockets to Protocol Switch

This page contains a table that allows you to enter a series of IP Port numbers and X.25 Call strings as shown below. It is used to configure the unit so that IP data can be switched to any of the protocols support by the protocol switch includingX.25. For example data that is received on a TCP connection can be forwarded over SSL, XoT or a UDP stream. The only columns that must be filled out are “Port” and “Number of Sockets”.

This table is duplicated in the ***Configuration - Network > Legacy Protocols > X.25 > IP to X.25 Call*** section as it can also be used to convert an incoming TCP connection to an X.25 session to be answered by PAD without using the protocol switch. It is included at this point in the web user interface as a convenience in case the table is being used in conjunction with PAD and not the protocol switch.



IP Port
The IP Port field is used to setup the port numbers for those IP ports that will “listen” for incoming connections that are to be switched over X.25 or other protocol. In the case of switching to X.25, when such a connection is made the unit will make an X.25 Call to the address specified in the X.25 Call field. Once this call has been connected, data from the port will be switched over the X.25 session.

Number of Sockets
The Number of Sockets field is used to select how many IP sockets should simultaneously listen for data on the specified port. The number of available IP sockets will depend on the model you are using and how many are already in use (see note below).

X25 Call
The X.25 call field may contain an X.25 NUA or NUI or one of the X.25 Call Macros defined on the ***Configuration - Advanced applications > X25 > Macros page***.

PID
The PID (Protocol Identifier), field specifies the PID to use when the unit switches an IP connection to X.25. The PID (protocol ID) field takes the format of four hexadecimal digits separated by commas, e.g. 1,0,0,0, at the start of the Call User Data field in the X.25 call.

Confirm Mode
When confirm mode is set to “On” then the incoming TCP socket will not be successfully connected until the corresponding outgoing call has been connected. The incoming TCP socket will trigger the corresponding outgoing call either to a local PAD instance or to whatever is configured. The effect of this mode is that the socket will fail if the outbound call

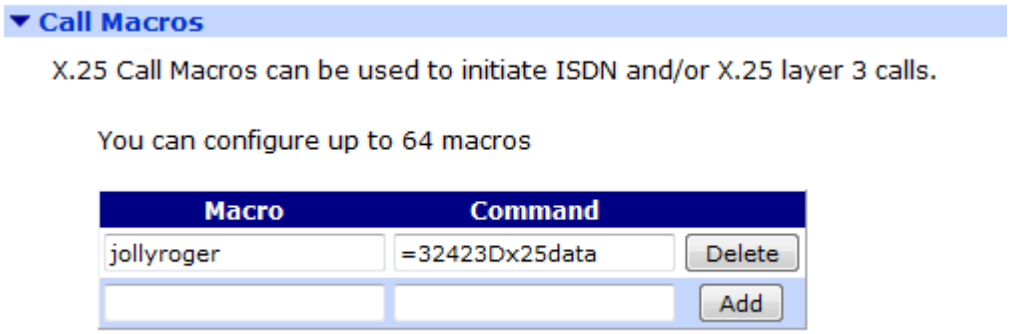
fails and so may be useful in backup scenarios. In addition it will ensure that no data is sent into a "black hole". (When this setting is not enabled data that is sent on the inbound TCP connection before the outbound connection has been successful can be lost.)

RFC 1086 Mode:
RFC 1086 specifies a mode of operation in which the IP socket answers and then with a simple protocol in the socket identifies the X.25 address and other X.25 call setup parameters to be used. Then when the X.25 call parameters have been identified the X.25 call is made and if successful then data is then switched between the X.25 call and the IP socket. The protocol will select whether incoming or outgoing support is required.

IP length header

When IP length header is "On", the IP length indicator field is inserted at the start of each packet. When set to "8583 Ascii 4 byte", the IP length header will conform to the ISO 8583 format.

In the example above, 3 IP sockets will "listen" for an incoming connection on IP Port 2004. Once connected they will each will make an X.25 Call to "jollyroger". The unit will recognise that "jollyroger" is a pre-defined macro (as illustrated below), and will translate it into an X.25 Call to address 32423 with the string "x25 data" included as data in the call. The outgoing X.25 call(s) will be made over whichever interface is specified by the Switch from XOT(TCP) to parameter on the ***Configuration - Network > Protocol Switch*** page.



Note:
At the top of the page the total number of sockets available and the number currently free is shown. Care should be take not to allocate too many of the free sockets unless you are confident that they are not required for other applications.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ipx25	n	ip_port	0 - 65535	IP Port
ipx25	n	nb_listens	0 – software dependant max	Number of Sockets
ipx25	n	x25call	NUA, NUI or X.25 macro name	X25 Call
ipx25	n	pid	hex numbers	PID
ipx25	n	cnf_mode	1 = enabled, 0 = disabled	Confirm Mode
ipx25	n	rfc1086_mode	1 = enabled, 0 = disabled	RFC 1086 Mode

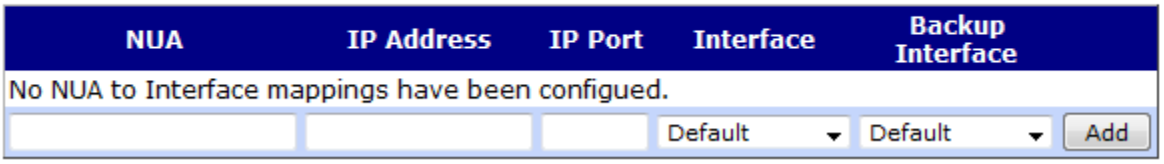
Entity	Instance	Parameter	Values	Equivalent Web Parameter
ipx25	n	iphdr	0=Off 1=On 2=8583 Ascii 4 byte	IP length header

NUA to Interface Mappings

Configuration - Network > Protocol Switch > NUA to Interface Mappings

This page contains a table that allows you to enter a series of X.25 NUA or NUI values along with IP addresses/Ports to which they should be mapped if you need to override the default settings in the Configuration - Network > Legacy Protocols > X.25 > NUA/NUI Interface Mappings page.

(You can specify up to 256 NUA to Interface mappings)



So, if in the Protocol Switch configuration you had configured the unit to switch from LABP 0 to TCP, the IP Address and Port values would normally be determined from the XOT Remote IP address and IP stream port parameters. However, having set up the NUA/NUI to IP addresses table as shown in the example above, if an X.25 call with NUA of value “222” is received on LAPB 0 it will be switched onto a TCP socket using IP address “1.2.3.4” on port 45 instead of those settings configured on the Configuration - Network > Legacy Protocols > X.25 > NUA/NUI Interface Mappings page.

Similarly, NUIs can also be matched and in this example a call with NUI of value “test” will be switched onto a TCP socket using IP address “100.100.100.1” on port 678.

All 3 comparison fields, NUA, NUI and Call Data, can use the wildcard matching characters “?” and “*”. In the example shown above when an X.25 call is received with either the NUA having “1234” followed by any 2 digits or a call being received with call user data with any 4 characters followed by “aa” then the call is switched to a TCP socket on address 100.100.100.52 on port 4001.

When a connection has been successfully established and data is being switched from the X.25 call to the socket and from the socket to the X.25 connection, it can be terminated by either the socket closing or the X.25 call clearing.

If the connection terminates because of an incoming X25 Call Clear packet then the switch will terminate the socket connection. If the connection terminates because the socket is closed then the switch will clear the X.25 call by transmitting a CALL CLEAR packet.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
nuaip	0-255	nua	0-65536	NUA
nuaip	0-255	ipaddr	IP address	IP Address
nuaip	0-255	ip_port	0-65536	IP Port
nuaip	0-255	swto	0-10, 12-15	Interface

Entity	Instance	Parameter	Values	Equivalent Web Parameter
			(see table below)	
nuaip	0-255	buswto	0-10, 12-15 (see table below)	Backup Interface

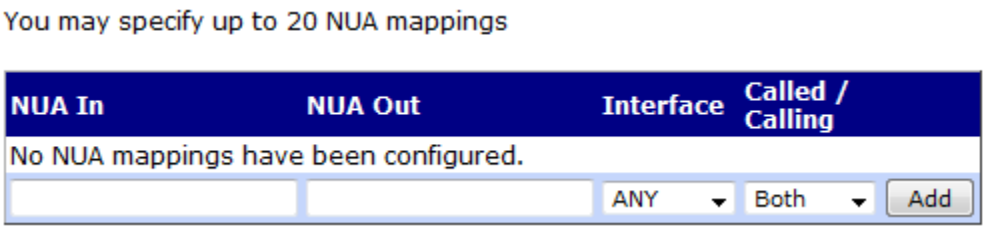
Interfaces are coded as follows:

Parameter Value	Interface Type
0	Default
1	LAPD
2	LAPB 0
3	LAPB 1
4	XOT
5	LAPD X (actual instance determined by NUA)
6	LAPB 0 PVC
7	LAPB 1 PVC
8	XOT PVC
9	TCP stream
10	UDP stream
12	LAPB 2
13	LAPB 2 PVC
14	VXN
15	SSL

NUA Mappings

Configuration - Network > Protocol Switch > NUA Mappings

Protocol switch NUA mappings allow you to redirect specified NUAs to alternative NUAs for switched X.25 calls. Up to twenty “NUA In” to “NUA Out” mappings are available. These mappings alter the called NUA field in any X.25 call. The comparison uses “tail” matching, so that only the rightmost digits in the NUA are compared with the table entry.



This page displays a table with four columns in which you can specify the NUA In values, corresponding NUA Out values, to which interfaces the mappings should be applied, and whether the mapping should apply if the unit is making the call, receiving the call, or both. For example, if the called NUA is 123456789345 and there is an NUA In table entry of 9345, with Called/Calling set to either “Both” or “Called”, then this will match, and the entire called NUA will be replaced with the corresponding NUA Out entry. In each case the interface type to which the mapping applies can be selected from “ANY”, “LAPD”, “LAPB0”, “LAPB1” “LAPB2” or “XOT”.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
X25map	0-19	nuafrom	0-65536	NUA In
X25map	0-19	nuato	0-65536	NUA Out
X25map	0-19	interface	0,1,2,3,4,12 0=Any 1=LAPD 2=LAPB 0 3=LAPB 1 4=XOT 12=LAPB 2	Interface
X25map	0-19	ca_or_ci	0,1,2 0=Both 1=Called 2=Calling	Called / Calling

Alarms Configuration

Configuration -Alarms

The ***Configuration -Alarms*** page has the following menu options:

Event Settings

Event Logcodes

SMTP Account

Event Settings

Configuration - Alarms > Event Settings

The router maintains a log of events in the "LOGCODES.TXT" pseudo file. When an event of a specified (or lower priority) level occurs, a syslog message, an email alert or SMS alert (on W-WAN models) can be sent to a pre-defined address. The ***Configuration > Alarms > Event Settings*** menu has the following sub-menuitems:

- Email Notifications
- SNMP Traps
- SMS Messages
- Local Logging
- Syslog Messages
- Syslog Server n

The ***Configuration > Alarms > Event Settings*** folder opens to show the following parameters:-

Only log events with a log priority of at least n
This parameter enables a filter that ensures that only events having a specified severity or lower level are logged.

Do not log the following events
This is a numerical list of comma-separated values specifying events to be excluded from the log. These numerical values can be found in the eventlog.txt file on the router.

After power up, wait s seconds before sending Emails, SNMP traps, SMS or Syslog messages
This parameter specifies the delay, in seconds, after power-up that the router should wait before sending any alert messages. This is useful in circumstances where the sending of those items would fail if sent too soon after the unit powers up because the underlying interface that would be used has not completed initialisation.

Include event number in the event log and Email, SNMP traps or Syslog messages
When this option is enabled, event numbers from the "logcodes.txt" file will be included.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
event	n	loglevel	0 – 9 0 none 1 low 9 high	Only log events with a log priority of at least n

Entity	Instance	Parameter	Values	Equivalent Web Parameter
event	n	ev_filter	Comma separated list of event numbers	Do not log the following events
event	n	action_dly	Number of seconds (e.g. 60)	After power up, wait s seconds before sending Email, SNMP traps, SMS or Syslog messages
event	n	incevnums	0,1	Include event number

Email Notifications

Configuration - Alarms > Event Settings> Email Notification

To use the email alert facility, you must first ensure that a valid Dial-out number, Username and Password have been specified and that the SMTP parameters have been set correctly. The Dial-out number, Username and Password parameters are to be found in the ***Configuration – Network > Interfaces > Advanced > PPP n*** pages where n is the relevant interface number.

The SMTP parameters are to be found under ***Configuration – Alarms > SMTP Account***.

Send email notifications
This checkbox simply enables the display of the configurable parameters when checked.

Send an email notification when the event priority is at least n
This is the lowest priority event that will generate an email alert message. For example, if this value is set to 6, only events with a priority of 6 or lower (7, 8 or 9) will trigger an automated email alert message. To disable email alarms, set this value to 0.

Send a maximum of n emails per day
This parameter sets the limit on the number of emails that may be sent during any 24 hour period. The intention is to prevent excessive alerts being sent when the event trigger value is set to a high priority / low value (1, 2 or 3 for example), i.e. a value that results in a large number of automated email alert messages being generated.

n emails have been sent today
This is a status message, indicating how many emails have been sent during the last 24 hour period.

Use email template file
This field contains the name of a template file that will be used to form the basis of any email alert messages generated by the event logger. The default template is a file called “EVENT.EML” that is stored within the compressed .web file. Alternative templates may be created, but in order to be valid, these must have the “.EML” file extension and be stored in the normal file directory. A new template having the name “EVENT.EML” will take precedence over the predefined “EVENT.EML” template but it is recommended that a new name is used, such as “event1.eml”.

Email To
This text field is the standard email address format for the intended recipient of the alert.

Email From
This text field should contain a valid email address that will be accepted by the SMTP server as being authorised to send email.

Email Subject
This text field should contain a short description of the email content.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
event	n	etrig	0 – 9 0 disables sending alerts	Send an email notification when the event priority is at least n
event	n	emax	0 – 255	Send a maximum of n emails per day
event	n	etemp	The name of a template file. Default is EVENT.EML	Use email template file
event	n	to	A valid email address, e.g. you@yourdomain.com	Email To
event	n	from	A valid email address	Email From
event	n	subject	A brief description of the content of the email	Email Subject

SNMP Traps

Configuration > Alarms > Event Settings> SNMP Traps

The router firmware supports the use of SNMP, with the ability to generate traps. In order for this facility to function, a SNMP trap server will need to be configured. SNMP trap server configuration is to be found under ***Configuration – Remote Management > SNMP > SNMP Traps***.

Send SNMP Traps
This checkbox, when checked enables the display of the following parameters:

Send a SNMP Trap when the event priority is at least n
This is the lowest priority event that will generate an SNMP trap message. For example, if this value is set to 6, only events with a priority of 6 or lower (7, 8 or 9) will trigger an automated SNMP trap message. To disable SNMP traps, set this value to 0.

Send a maximum of n SNMP taps per day
This parameter sets the limit on the number of emails that may be sent during any 24 hour period. The intention is to prevent excessive alerts being sent when the event trigger value is set to a high priority / low value (1, 2 or 3 for example), i.e. a value that results in a large number of SNMP trap messages being generated.

n SNMP traps have been sent today
This is a status message, indicating how many SNMP trap messages have been sent during the last 24 hour period.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
event	n	trap_trig	0 – 9 0 disables sending alerts	Send a SNMP Trap when the event priority is at least n

Entity	Instance	Parameter	Values	Equivalent Web Parameter
event	n	trap_max	0 – 255	Send a maximum of n SNMP traps per day

SMS Messages

Configuration > Alarms > Event Settings> SMS Messages

Note:
This option is only available on routers with W-WAN capability.

This section has three identical rows, each of which controls the setting of the SMS alert messages.

Send SMS messages to
This field should contain the destination telephone number (MSISDN) for SMS alert messages. The format for this field is the international dialling code followed by the number, but should not contain a '+' prefix. For example, UK mobile 07871 445677 would be 447871445677

If the event priority is at least n
This numeric input field sets the trigger level for the alert message. If, for example, this field is set to the value 6, only events having a priority of 6 or higher will trigger an automated SMS alert. Setting this field to 0 disables the sending of SMS alerts.

Use SMS template
This field contains the name of the template file that will be used to form the basis of any alarm messages generated by the event logger. The default template file is a test file called "EVENT.SMS" that is stored in the compressed .web file. A new template may be created, and if named "EVENT.SMS" will take precedence over the pre-defined "EVENT.SMS" template but it is recommended that a new name is used, such as "event1.sms". Templates should use the ".SMS" file extension.

Send a maximum of n SMS messages per day
This parameter limits the number of SMS alert messages sent by the router in any one day.

n SMS messages have been sent today
This is a status message, indicating how many SMS alert messages have been sent during the last 24-hour period.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
event	n	sms_to	A valid mobile number e.g. 447871445677	Send SMS messages to
event	n	sms_trig	0 – 9	If the event priority is at least n
event	n	sms_to2	A valid mobile number e.g. 447871445677	Send SMS messages to
event	n	sms_trig2	0 – 9	If the event priority is at least n
event	n	sms_to3	A valid mobile number e.g. 447871445677	Send SMS messages to
event	n	sms_trig3	0 – 9	If the event priority is at least n
event	n	sms_temp	event.sms (template	Use SMS template

Entity	Instance	Parameter	Values	Equivalent Web Parameter
			file stored in the compressed .web file)	
event	n	sms_max	0 – 255	Send a maximum of n SMS messages per day

Local Logging

Configuration > Alarms > Event Settings> Local Logging

A secondary log file can be created on a USB flash drive and events will be appended to this log file. This facility is useful if an extended logging period is required where, the normal eventlog.txt file would overwrite early events before the operator has had a chance to view them. The secondary log file can be limited in size or allowed to fill the USB flash drive. Once the log file is full, earlier events will be pruned from the end of the file to allow new events to be added.

Local Drive to log to
This parameter determines the drive letter where the USB flash drive is located. This is designated "u" for a USB drive.

Log filename
This specifies the name of the file for the secondary event log.

Log size
This field specifies the maximum size of the log file in kilobytes.

XML logs
On platforms that support it, event logs can be saved in XML format. This field specifies the size of the XML log file in kilobytes. The files created will be named EVXML1.XML, EVXML2.XML etc.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
event	n	logdrive	Drive letter, e.g. "**u**" for USB flash drive	Local drive to log to
event	n	logfile	Name of the file e.g. mylog.txt	Log filename
event	n	logsizek	Size of log in kilobytes e.g. 1048576 Which is 1MB	Log size
event	n	xmllogs		None

Syslog Messages

Configuration > Alarms > Event Settings> Syslog Messages

As well as logging events to an internal log file and to a file on a USB flash drive, the router can log events to a Syslog server.

This section describes how to configure the router to send Syslog messages to a Syslog server.

Send Syslog messages
When this checkbox is checked, the following options are displayed:

Send a Syslog message when the event priority is at least n
This is the lowest priority event that will generate a syslog message. For example, if this value is set to 6, only events with a priority of 6 or lower (7,8 or 9) will trigger an automated syslog message. To disable syslog messages, set this value to 0.

Send a maximum of n Syslog messages per day
This parameter sets the limit on the number of syslog messages that may be sent during any 24 hour period. The intention is to prevent excessive alerts being sent when the event trigger value is set to a high priority / low value (1, 2 or 3 for example), i.e. a value that results in a large number of syslog messages being generated.

n Syslog messages have been sent today
This is a status message that indicates how many Syslog messages have been sent in the last 24 hour period.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
event	n	syslog_trig	0 – 9	Send a Syslog message when the event priority is at least n
event	n	syslog_max	0 - 255	Send a maximum of n Syslog messages per day

Syslog Server n

Configuration > Alarms > Event Settings> Syslog Server n

This section describes the configuration of the router for defining the Syslog server to send messages to.

Syslog server IP address
This parameter sets the IP address of the server.

Port
This parameter sets the port to use.

Note:
The following three items (Mode, TCP timeout and Route) only appear on routers that have the TCP logging software option enabled. This is not a commonly used option.

Mode
There are currently three supported communication modes, these are selected from a drop-down list and are TCP, UDP and a protocol described in RFC 3195.

TCP timeout s seconds
For TCP communications, this parameter sets the timeout on the socket.

Route using
These radio buttons selects which method of establishing a route to the server should be used.

Routing table
When this radio button is selected, the routing table is used to determine the interface that will be used to transmit the syslog message.

Interface x,y

If the routing table is not to be used, an interface type (PPP or Ethernet) may be selected from the drop-down selection box and the interface instance number may be typed into the adjoining text entry box. The route is then determined by that interface.

Priority

The checkboxes listed in this section select the event priorities that should cause the event to be logged.

Facility

The checkboxes listed in this section select which of the router facilities should be logged.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
syslog	n	server	IP address	Syslog server IP address
syslog	n	port	IP port number	Port
syslog	n	mode	UDP, TCP, RFC3195	Mode
syslog	n	tcp_to	Timeout in seconds, e.g. 86400	TCP timeout s seconds
syslog	n	source_ent	PPP, ETH	Interface x,y x = Interface type
syslog	n	source_add	0 - 4	Interface x,y y = interface number
syslog	n	priority	Hyphen separated 0 – 7 Comma separated 0,3,5 or 'all'	Priority checkboxes
syslog	n	facility	Hyphen separated 0 – 23 Comma separated 4,3,5,10,15,22 or 'all'	Facility checkboxes

Event Logcodes

Configuration - Alarms > Event Logcodes

This page allows you to edit the logcodes used to describe events entered in the "EVENTLOG.TXT" pseudo file. If a change is made to the logcodes.txt file, the changes will be saved in the file logcodes.dif so when a firmware upgrade is performed the changes to the logcodes are retained.

The page that appears under the blue bar initially shows a table containing the Event descriptions and reason. Clicking on an item shown in bright blue (an HTML link) causes a configuration page associated with that item to be opened. The newly-opened page allows that item to be configured. The configuration options shown on that page are described below.

Event

This is not a configurable parameter; it is simply the event number, displayed for information only. This is the number to refer to when filtering events in the event log settings ***Configuration – Alarms > Event Settings***.

Description
This field is a description of the event code. Clicking on a link in this field brings up the configuration page associated with that event.

Filter
This parameter is for information only. If event filtering is applied to an event, the associated filter is shown as "On". This is a result of enabling the parameter 'Do not log this event' as described below.

Event Priority
This parameter controls the priority of the event and is used to determine whether an event will trigger email, SMS messages or SNMP traps.

Reasons
The reason why the event occurred. Not every event has a list of reasons.

Reason Priority
This parameter is for information only.

Attachment List ID
This is just a fixed list of values that may be used to conveniently refer to the associated list of files to attach to an email.

Files
This text entry box allows the user to type in a comma-separated list of names for the files that should be attached to an email.

Configuring Events

This page controls the configuration of the event that is displayed in bold font at the top of the page, just below the blue title bar.

Do not log this event
When checked, this checkbox disables logging of the event.

Note:
This parameter is **not** saved in the logcodes.txt file but in the config.dan file. This means that after changing this parameter, the changes must be saved by clicking the save changes link when prompted (this appears after clicking the "Apply" button). Clicking the Save All Event Code Changes will not have the desired effect.

Log Priority
This parameter sets the priority of the event to determine whether the event will trigger emails, SMS messages or SNMP traps. 0 = disabled, 1 = highest priority, 9 = lowest priority

Alarm Priority
If the above "Inherit alarm priority from event" checkbox is **not** checked, this parameter selects the priority of the reason. Valid values are 0 to 9.

Alarm Priority is dependent on the event being logged by Entity
Selecting this checkbox makes the priority conditional on which system entity triggered the event (e.g. ethernet) and enables the following two configuration options:

Entity

This drop-down selection box contains a list of the system entities.

All
Selecting this radio button causes all of the system entities

Instance
Selecting this radio button enable a text entry box that allows the user to enter the instance of the selected entity.

Priority only applies to
This configuration section comprises a set of checkboxes, each checkbox controlling whether the priority is applied to that interface instance. So for example, to apply the priority to PPP interface 1, click on the checkbox labelled PPP 1.

Store a snapshot of the Traffic Analyser trace on the log drive
Selecting this checkbox causes a snapshot of the analyser trace to be stored on the USB flash drive

If this event creates an Email alarm

Attach a snapshot of the Traffic Analyser trace
Checking this checkbox will cause a snapshot of the analyser trace to be attached to the email.

After this event

Leave the Analyser trace
This option will leave the analyser trace unchanged.

Freeze the Analyser trace
This selection will cause the analyser to be “frozen”, i.e. no more logging will take place until the email has been sent.

Delete the Analyser trace
This selection will cause the analyser trace to be deleted once the email has been sent.

Attach a snapshot of the Event Log
Selecting this checkbox will cause the eventlog to be attached to the email.

After this event

Leave the Event Log
Selecting this radio button will leave the event log unchanged.

Delete the Event Log
Selecting this radio button will cause the event log to be deleted after the email has been sent.

Attachment List ID
This text entry box allows the user to specify which files to attach to the email. The ID refers to the table of files.

Syslog Priority
This drop-down selection box contains the following options:
Emergency, Alert, Critical, Error, Warning, Info, Debug

Syslog Facility
This drop-down selection box contains the following options:
Kernel, User, Mail, System, Auth, Syslog

Configuring Reasons

The page invoked by selecting a reason link in the event logcodes table is very similar to the Configuring Events page but with the following differences.

There is no “Do not log this event” checkbox. There is the following additional parameter:

Inherit alarm priority from event
Selecting this checkbox causes the following “Alarm Priority” parameter to be disabled and cause the priority to be the same as the event that triggered it. The “Alarm Priority” parameter is the same as in the “Configuring Events” page.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
event	n	ev_filter	Comma separated list of event codes	Do not log this event

There are no CLI commands for editing Event logcodes. However, it is possible to edit the “LOGCODES.TXT” file which holds all the logcode information. For details on how to do this, refer to the “Event Log” section of this manual.

SMTP Account

Configuration - Alarms > SMTP Account

In order for the router to successfully send emails, an email account (SMTP) must be available. This section describes the configuration of the router in order to use the email account that has been set up for it.

Hostname or IP address of your SMTP server

This parameter sets the IP address or hostname of the SMTP mail server, e.g. smtp.myisp.com. Sending email requires a connection to the Internet so depending upon how the router is configured, it may be necessary to check that the PPP configuration allows a connection to the ISP or external SMTP mail server.

Port

The Simple Mail Transfer Protocol (SMTP) uses TCP port 25, which is the default for this parameter. If the mail server uses a different TCP port, enter it here.

Username

Email accounts are controlled by requiring a username and password in order to send and receive mail. This field is where the account username is set. This information will be provided by the administrator of the email server.

Password

This field is where the account password is set.

Confirm Password

This field is used to re-enter the password. The two passwords are compared to check that they are the same and that there hasn’t been a typographical error when entering them. This check is used since the password characters are not echoed and so the usual visual feedback is not available.

Display “Email From” as

This parameter specifies the text to be used as the “MAIL FROM” parameter which forms part of the protocol when connecting to the email server. Most SMTP servers will accept an empty string whereas others require that this parameter is present. It may be necessary to consult with the SMTP server administrator (or ISP) to determine whether or not this parameter is required.

Attachment size limit n Kbyte, Mbyte

Some email service providers place a limit on the size of an email attachment that they will accept, this parameter can be used to ensure that the limit is not exceeded. The inbuilt traffic analyser and event logger can generate substantial files and it may be required that these files are truncated when sent as email attachments. The size is specified in kilobytes, so for example, setting this limit to 250 will truncate the attachment to 250kB before transmission. Setting the size to 0 means that no limits are imposed.

If the email template does not contain one, use “Reply To” address

This address will be inserted into the email header if it is found that no reply address exists in the appropriate email template. If the email template does contain an address in the “reply to:” field, that will override the default reply address.

Route using Routing table, Interface x,y

When selected, the routing code is used to determine the outbound interface and that interface will determine the source IP address.

If the “Route using routing table” option is not selected, the settings in the interface and interface instance text boxes are used to determine the outbound interface and source IP address. These are selected from the drop-down selection box and are None, PPP and Ethernet.

Resend the email after s seconds if the first attempt fails

This checkbox and associated text entry box enable the retry mechanism. If the first attempt to deliver the email fails, the router will wait the specified number of seconds (which must be non-zero) before making another attempt.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
smtp	n	server	Valid hostname or IP address	Hostname or IP address mailserver.isp.com 122.134.156.178
smtp	n	port	Valid port number, e.g. 25	Port n
smtp	n	username	Free text field containing a valid account username e.g. my_account	Username
smtp	n	password	Free text field containing account password, e.g. my_password	Password

Entity	Instance	Parameter	Values	Equivalent Web Parameter
smtp	n	mail_from	Free text field	Display “Email From” as
smtp	n	att_lim	0 – 65535	Attachment size limit This CLI value is entered in Kilobytes only.
smtp	n	reply_to	Free text field	If the email template does not contain one, use "Reply To" address
smtp	n	userouting	0,1	Route using routing table
smtp	n	ll_ent	Blank,PPP,ETH	Route using Interface x,y x = Interface type
smtp	n	ll_add	0 - 255	Route using Interface x,y y = interface number
smtp	n	retry_dly	0 - 255	Resend the email after s seconds if the first attempt fails

Systems Configuration

The ***Configuration – Systems*** menu has the following sub-menu options:

- Device Identity
- Date and Time
- General

Device Identity

Configuration – Systems > Device Identity

This configuration section describes how to configure the identity of the router.

Description
This free-form text input field is for entering a description of the router that can be used to uniquely identify it. This is useful where there are a large number of routers on a site and a descriptive name would be easier to use when referring to the router, rather than having to use the serial number or other unique parameter. This parameter is used by the SNMP function within the router.

Contact
This is another SNMP parameter which is used to enter a contact name.

Location
This SNMP parameter sets a location string for the router, which again may be helpful when referring to a particular router within a site or for identifying a particular site.

Device ID
This field is taken from the device cloud configuration and should not normally need to be changed. When using device cloud to manage the router, the configuration procedure assigns a device ID to the router. The device ID is a 64-byte value, with each 8-byte section separated with a "-" character. Valid digits are upper case hexadecimal. The first 16 digits (reading from left to right) are normally set to "0" and the second 16 comprise the MAC address of the primary Ethernet interface and the digits "FF" in order make up the full 8-digit. The following device ID illustrates the format:

00000000-00000000-001122FF-FF334455

This example uses the MAC address 00:11:22:33:44:55.

Router Identity
This is a string of up to 20 characters that can be used to identify the router in email alert messages generated by the event logger. This is also the prompt string that appears when logging on to the router remotely. The factory configuration uses the character sequence "%s" which gets replaced by the serial number of the router when the unit identity is displayed. This character sequence may be used when creating a custom identity for the router. For example, if the serial number of the router is **012345**, entering the string "**My_Router_%s>**" would show the prompt "**My_Router_012345**>" during a remote login.

Hostname
This parameter assigns a hostname to the local IP address of the router.

Secondary Hostname
This parameter allows a second hostname to be assigned to a router. This is associated with the secondary IP address.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snmp	n	Name	Free text field	Description
snmp	n	Contact	Free text field	Contact
snmp	n	Location	Free text field	Location
cmd	n	Unitid	Free text field	Router Identity
cmd	n	Hostname	Free text field	Hostname
cmd	n	sec_hostname	Free text field	Secondary Hostname

Date and Time

Configuration – Systems> Date and Time

The router keeps track of calendar time using an internal real time clock (RTC) device. The clock is used to time/date stamp logfiles. The date and time configuration pages allow the system time to be set and maintained. Since maintaining an accurate system clock can be important for routers on the Internet, NTP and SNTP services are supported and the router may be configured to use one of these protocols for maintaining the internal system time. The router uses the 24-hour clock.

Current system time

The current system time appears at the top of this web page.

Manually set the time h hours, m minutes s seconds, M month D day Y year

These parameters are set using the associated drop-down selection menus.

Hours

Select from the drop-down list to set the hours.

Minutes
Select from the drop-down list to set the minutes.

Seconds
Select from the drop-down list to set the seconds.
(This may have limited use due to human reaction times).

Month
Select from the drop-down list to set the month.

Day
Select from the drop-down list to set the day.

Year
Select from the drop-down list to set the year.

Set
Click this button to cause the above settings to take effect.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
n/a	n/a	time	hh [mm [ss [DD [MM [YYYY]]]]]	Manually set the time

Autoset Date and Time

Do not auto-set the system time
This is the system default and this radio button will appear filled in when the unit is new unless a different default configuration has been supplied. Click this radio button to close the SNTP or NTP configuration pages.

Auto-set the system time
Selecting this radio button expands the page to include the SNTP settings. These are described below.

SNTP server
The hostname or IP address of the desired SNTP server is entered here.

Check on Power-up
This checkbox, when checked, will cause the router to attempt to connect to the SNTP server every time it boots.

Update every h hours
Enter the interval, in hours that the router should wait between updating the system clock.

Randomly between s1 and s2 seconds
It is possible to use a random update interval rather than a fixed interval. There are two text-entry boxes for this purpose, enter the minimum interval into the left-hand box and the maximum desired interval into the right-hand box. Selecting the random update will clear the fixed interval.

Offset from GMT
This parameter should be set to + or - the number of hours the unit's time should be ahead or behind Greenwich Mean Time.

Update for Daylight Saving Time.
When checked, this checkbox causes the following parameters to appear, the router will then use those settings to automatically adjust the system time to ensure that local daylight saving is used.

Start

Month
Use this drop-down selection box to select the month in which to switch to daylight saving time.

Day
Use this drop-down selection box to select the day on which to switch to daylight saving time.

Hour
Use this drop-down selection box to select the hour at which to switch to daylight saving time.

End

Month
Use this drop-down selection box to select the desired month in which to switch back to GMT (UTC).

Day
Use this drop-down selection box to select the desired day on which to switch back to GMT.

Hour
Use this drop-down selection box to select the desired hour at which to switch back to GMT.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
sntp	n	server	Valid hostname or IP address sntp.timeserve.org	SNTP Server
sntp	n	pwrchk	0,1	Check on Power-up 0 = Off 1 = On
sntp	n	interval	0 – 255	Update every h hours Default = 24
sntp	n	randintsecs	0 - 86400	randomly between s1 and s2 seconds Use format [s1,s2] eg min 50, max 500 would be: [50,500]
sntp	n	offset	-12 - +13	Offset from GMT
sntp	n	dstonmon	0 – 12	Start: Month Update for Daylight Saving Time 0 disables daylight saving
sntp	n	dstonday	0 - 31	Start: Day
sntp	n	dstonhr	0 - 23	Start: Hour
sntp	n	dstoffmon	0 - 12	End: Month
sntp	n	dstoffday	0 - 31	End: Day
sntp	n	dstoffhr	0 - 23	End: Hour
sntp	n	ntp	0,1	0 = SNTP 1 = NTP Default = OFF

Use NTP for greater accuracy
Selecting this checkbox expands the page to show the NTP settings. These are described below.

NTP is much more accurate than SNTP, with NTP an accuracy of 200 microseconds (1/5000 second) can be achieved. The NTP functionality is in accordance with RFC1305.

Up to 4 remote peers can be configured, all the peers are polled at intervals and the “best” peer is selected for using as the time source.

SNTP should be configured prior to using NTP. The router will calculate the accuracy of the NTP time servers over a period of time (up to 2 hours), once the drift compensation is calculated the NTP client will be used.

The drift compensation value will be stored in NVRAM and written to the config.da0 file, if the router looses power or is rebooted it will not need to re-calculate the accuracy of the NTP servers again. The compensation value is constantly monitored to ensure it remains correct.

Note:
If SNTP is used the accuracy of around 1 second is achieved.
If NTP is used 200 microsecond accuracy can be achieved.
Not all models support NTP – this option will only appear for models that do.

Initial Drift Compensation n ppm
NTP incorporates compensation for clock drift. If this parameter is known, it can be entered here. Otherwise, the router will calculate this value over a period of time. Once calculated, the value will be displayed in the text box.

Clock Precision Limit

Select the clock precision limit from the drop-down selection box.

Disable NTP when interface x,y is out of service

If the specified interface is out of service, the NTP is disabled until the interface is available again.

NTP Servers 1 - 4

The router has the capability of configuring up to four NTP server connections. The more servers that are used, the more accurate the time setting will be. The following section describes the configuration of the connections.

NTP Server 1/2/3/4 Hostname
This field sets the NTP server hostname or IP address.

Broadcast Mode
When enabled, the NTP client will operate in a different manner. Rather than sending out an NTP client message and expecting a reply, the NTP module will send out a broadcast mode packet to the IP address configured in 'NTP host' field. The broadcast interval will be determined by the value of 'Minimum poll interval'.

Poll Interval s1 to s2 seconds
These two parameters define the minimum and maximum intervals between poll broadcasts. The values are time in seconds represented as a power of 2. This means that a value of 4 means that the minimum poll interval is 2^4 = 16 seconds.

Startup burst Interval s seconds
When connecting to an NTP time server in polled mode, it may be necessary to send polls at intervals shorter than the minimum poll interval in order to speed up the synchronization process. This parameter controls the interval between polls during the startup process. This feature is useful in situations where the router only has an intermittent Internet connection.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ntp	n	driftppm	-10000 - +10000	Initial Drift Compensation
ntp	n	precision	-10 - 0	Clock Precision Limit
ntp	n	inhibit_int	Blank,PPP,Ethernet	Disable NTP when interface x,y is out of service x = Interface type
ntp	n	inhibit_add	0 - 255	Disable NTP when interface x,y is out of service

Entity	Instance	Parameter	Values	Equivalent Web Parameter
				y = interface number
ntp	n	server	Valid IP address or hostname, e.g. ntp1@timeserver.org	NTP Server
ntp	n	bcast	0,1	Broadcast Mode 0 = disabled 1 = enabled
ntp	n	minpoll	3 - 14	Poll Interval s1, s2 3 = 8 4 = 16 5 = 32 6 = 64 7 = 128 8 = 256 9 = 512 10 = 1024 11 = 2048 12 = 4096 13 = 8192 14 = 16384
ntp	n	maxpoll	3 – 14	Poll Interval s1, s2 See 'minpoll' for values
ntp	n	burstint	0 – 255	Startup burst Interval s seconds
ntp	n	server2	Valid IP address or hostname, e.g. ntp2@timeserver.org	NTP Server
ntp	n	bcast2	0,1	Broadcast Mode 0 = disabled 1 = enabled
ntp	n	minpoll2	3 - 14	Poll Interval s1, s2 See 'minpoll' for values
ntp	n	maxpoll2	3 - 14	Poll Interval s1, s2 See 'minpoll' for values
ntp	n	burstint2	0 – 255	Startup burst Interval s seconds
ntp	n	server3	Valid IP address or hostname, e.g. ntp3.timeserver.org	NTP Server
ntp	n	bcast3	0,1	Broadcast Mode 0 = disabled 1 = enabled
ntp	n	minpoll	3 - 14	Poll Interval s1, s2 See 'minpoll' for values

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ntp	n	maxpoll	3 - 14	Poll Interval s1, s2 See 'minpoll' for values
ntp	n	burstint3	0 – 255	Startup burst Interval s seconds
ntp	n	server4	Valid IP address or hostname, e.g. ntp4.timeserver.org	NTP Server
ntp	n	bcast4	0,1	Broadcast Mode 0 = disabled 1 = enabled
ntp	n	minpoll4	3 - 14	Poll Interval s1, s2 See 'minpoll' for values
ntp	n	maxpoll4	3 - 14	Poll Interval s1, s2 See 'minpoll' for values
ntp	n	burstint4	0 – 255	Startup burst Interval s seconds

To check the status of the NTP client, the following commands can be used:

To view NTP system status information

ntpstat sys

To view NTP peer information

ntpstat peers

To reset system information and allow NTP to recalculate the drift compensation

ntpstat rst

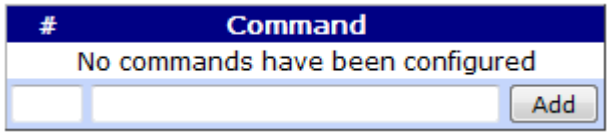
General

Configuration – Systems> General

This section describes the configuration of router functionality that applies to the router in general rather than specific features.

Autorun Commands

The router may be configured to run a number of commands once it has booted. These commands are associated with specific asynchronous serial interfaces. Configuration of this facility is via a table on this web page. As an example, it may be required that a Script Basic script, sample.bas needs to be run at boot up. Auto commands are normally associated with an ASY port, but running a script for example is not ASY port specific.



#
This parameter is the command interface to be associated with the command. In the above example, this would be set to the number "0".

<Command>
This parameter is the CLI command to run on start-up. In the above example, this field would be set to the string “bas sample.bas”.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
cmd	n	autocmd	Valid CLI command	Autorun Commands

Web / Command Line Interface

The router may be configured using several different methods. This section describes how to configure the web GUI and CLI (Command Line Interface) options.

Automatically log user out if idle for h hours m minutes s seconds
In order to limit the probability of unauthorised users gaining access to the router, login timeouts are applied. These cause an existing connection to be closed after a predefined period. The default is 20 minutes.

For users connected on the local Async port

Use access level None, Low, Med, High, Super
For security purposes, logging into the unit is controlled by a user access level. This parameter controls the access level that applies when logging in via the local asynchronous serial port.

Automatically log user out Never / If idle for h hrs m mins s secs
These radio buttons control how long the local port allows access before terminating the connection and requiring the user to log in again. Selecting the “Never” buttons allows permanent access to the router via the local asynchronous serial port. If, for security reasons, it is required that the access should be limited, the appropriate time period can be entered into the text entry boxes.

Disable Remote command echo for Telnet sessions
This checkbox enables/disables command echo for remote access. This applies to telnet and TRANSIP sessions.

CLI Pre-Login Banner
The router offers the facility to display a banner before any login information is requested. The parameter specifies the name of a file that is stored in the flash filing system and contains the text to be displayed before the request for the username and password. This can be useful for displaying a standard welcome message or any site-specific user instructions.

CLI Post-Login Banner
Once the user has successfully logged on to the router, a second message may be displayed - this parameter specifies the name of a file containing the text to display. As above, the file may contain site-specific instructions to be carried out once the user has logged in.

Allow CLI access from X.25 address n
This parameter enables/disables logging into the router over an X.25 connection. The paramtern n must be a valid X.25 NUA (Network User Address).

With TRANSIP, use access level None, Low, Med, High, Super
This drop-down selection box controls the security access level when using TRANSIP to access the router.

Relevant CLI Parameters

Entity	Instance	Parameter	Values	Equivalent Web Parameter
cmd	n	tremto	0 – 86400 seconds	Automatically log user out if idle for h hrs m mins s seconds This CLI value is entered in seconds only.
local	n	access	0 – 4	Use access level 0 = Super 1 = High 2 = Medium 3 = Low 4 = None 8 = Read only
local	n	tlocto	Free text field	Never, h hrs, m mins, s secs
cmd	n	noremecho	0,1	Enable Remote command echo 0 = Off (default) 1 = On
cmd	n	prebanner	Valid filename e.g. “welcome1.txt”	CLI Pre-Login Banner
cmd	n	postbanner	Valid filename e.g. “welcome2.txt”	CLI Post-Login Banner
cmd	n	cmdnua	0 - 1023	Allow CLI access from X.25 address
local	n	transaccess	0 – 4	With TRANSIP, use access level 0 = Super 1 = High 2 = Medium 3 = Low 4 = None 8 = Read only

Miscellaneous

This section is for those configuration items that do not fit neatly into any other section.

Note:
Depending on the router model, some of these options may not be available.

Use Config n when the router powers up
The router maintains two configuration files, either of which may be invoked on power-up. Select the required one from the drop-down selection box. Use this option with care as selecting the incorrect configuration file can cause confusion.

Allow anonymous FTP login
When checked, this checkbox will enable the router to accept anonymous logins. The default state is Off and the security implications of enabling this option should be considered carefully before applying.

Additional FTP NAT port n
Standard FTP uses two well-known ports, a control port and data port. These are low number ports and may be blocked by firewall rules. As such, it may be that an FTP server may be listening on a non-standard control port. This parameter is used to specify the port

that the router should monitor for the FTP “PORT” and ”PASV” commands. These commands contain information relating to IP addresses and Ports which should be modified during the NAT process. The NAT modifications may result in different sized packets being generated that then require that the TCP sequence numbers be modified to allow for the changes.

SNMP Enterprise number
This parameter specifies the value of the OID (Object IDentifier) to be used by SNMP management tools when accessing the MIB (Management Information Block). This number must form part of the OID used to access individual items in the MIB as a prefix.
For example: SNMPv2-SMI::enterprises.16378.10001.

SNMP Enterprise Name
This is the name corresponding to the above Enterprise Number.

Only resolve DNS request for domain
Entering a domain name here will restrict DNS requests to the specified domain only.

W-WAN LED to display W-WAN, ISDN/PSTN
On the front panel of the display of models fitted with a W-WAN module, is an LED that may be used to display the status of the W-WAN module or the status of the PSTN/ISDN connection. Use the drop-down selection box to choose which. The ISDN/PSTN settings depend upon which of these two options are available on the router.

Serial LED to display Connection, DTR
On the front panel of the router is an LED dedicated to indicating the status of various signals on the asynchronous serial line. Use the drop-down selection box to choose which signal status to display. On modules fitted with W-WAN, this LED has additional functionality, it can also be used to display the W-WAN signal strength.

CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
config	n	powerup	0,1	Use Config n when the router powers up
cmd	n	anonftp	0,1	Allow anonymous FTP login 0 = Off (default) 1 = On
snmp	n	ftpnatport	0 - 65535	Additional FTP NAT port
snmp	n	ent_nb	0 – 65535	SNMP Enterprise Number Default 16378
cmd	n	ent_name	Free text field	SNMP Enterprise Name
cmd	n	dnsname	Valid Domain name, e.g. mydomain.org	Only resolve DNS request for domain
cmd	n	gprsled_mode	0,1	W-WAN LED to display W-WAN, ISDN/PSTN 0 = W-WAN 1 = ISDN/PSTN
cmd	n	asyled_mode	0,1	Serial LED to display Connection, DTR 0 = Connection 1 = DTR status

Entity	Instance	Parameter	Values	Equivalent Web Parameter
				2 = W-WAN signal strength

Remote Management Configuration

The ***Configuration – Remote Management*** page has the following menu options:

- Device Cloud
- SNMP

Device Cloud

Configuration – Remote Management > Device Cloud

The ***Configuration – Remote Management > Device Cloud*** menu has the following sub-menu options:

- Connection Settings
- Advanced
- SMS Settings

Connection Settings

Configuration – Remote Management > Device Cloud > Connection Settings

Device Cloud is a hosted remote configuration and management system that has been designed to facilitate the management of large numbers of routers. Before this service can be used, a device cloud account must be set up. Applying for an account is a straightforward procedure; the local sales representative will have details. The Device Cloud homepage is to be found at ***www.etherios.com/devicecloud***.

The service is hosted on the device cloud servers and these provide a web-based interface that shows the configuration of selected routers allows the configuration to be changed and also facilitates remote firmware upgrade. The device cloud servers also provide a data storage facility.

Enable Remote Management using a client-initiated connection
Select this checkbox to display the basic configuration parameters and enable the unit to make the connection to the remote device cloud server.

Server Address
This text entry box is used to enter the IP address or (more usually) the domain name of the device cloud host, for example ***login.etherios.com***. (This information will be supplied when your device cloud account is activated).

Automatically reconnect to the server after being disconnected
The protocol used to communicate with the server allows the router to detect that it is no longer connected to the server. Ticking this checkbox will cause the router to attempt a reconnection when it discovers that the connection has been lost.

Reconnect after h hours m minutes s seconds
If the reconnect checkbox is enabled, these parameters specify the interval to wait before attempting to reconnect to the server.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
cloud	n	clientconn	0,1	Enable Remote Management and Configuration using a client-initiated connection 0 = Off

Entity	Instance	Parameter	Values	Equivalent Web Parameter
				1 = On
cloud	n	server	Valid IP address e.g. 1.2.3.4 or domain name e.g. login.etherios.com	Server Address
cloud	n	reconnect	0,1	Automatically reconnect the server after being disconnected 0 = Off 1 = On
cloud	n	reconnectsecs	0 – 86400	Reconnect after h, m, s This CLI value is entered in seconds only.

Advanced

Configuration – Remote Management > Device Cloud > Advanced

The settings in the previous section, along with the system defaults are sufficient to establish a connection to the device cloud server. The settings in the advanced section allow the connection to be fine-tuned. The parameters described here are concerned with detecting loss of connection. When the router first connects to the device cloud server, the link parameters are sent to it. The WAN settings and Ethernet settings described below are identical, but it should be noted in the command line descriptions that the default keepalive intervals are different. This is due to the different characteristics of PPP and Ethernet links.

Connection Settings

Disconnect when the device cloud server is idle
Once the router has connected to the device cloud server, and the server has established that all the settings it holds for the router are current, and no new changes are being requested, the traffic between the router and device cloud server reduces to the sending of keep-alive packets. In this situation, it may be advantageous to terminate the connection in order to reduce bandwidth or to keep data costs down. Ticking this checkbox will cause the router to negotiate termination of the connection.

Idle Timeout h hours, m minutes, s seconds
The timeout entered here defines how long the router should wait after detecting the idle condition before negotiating termination of the link. Default is 10 seconds.

WAN Settings

Receive Interval s seconds
This is the time between keep-alive packets that the router should wait before considering that the connection may be lost.

Transmit Interval s seconds
This is the interval between transmission of keep-alive packets.

Assume connection is lost after n timeouts

Occasional packet loss is to be expected, this parameter will allow for a specified number of lost keep-alive packets before the connection is deemed to have failed.

Ethernet Settings

Receive Interval s seconds
This is the time between keep-alive packets that the router should wait before considering that the connection may be lost.

Transmit Interval s seconds
This is the interval between transmission of keep-alive packets.

Assume connection is lost after n timeouts
Occasional packet loss is to be expected, this parameter will allow for a specified number of lost keep-alive packets before the connection is deemed to have failed.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
cloud	n	idledisconn	0,1	Disconnect when device cloud server is idle 0 = Do not disconnect 1 = disconnect
cloud	n	disconnsecs	0 - 28800	Idle Timeout h,m,s This CLI value is entered in seconds only.
cloud	n	ppprxkeepalive	0 - 28800	WAN - Receive Interval seconds
cloud	n	ppptrxkeepalive	0 - 28800	WAN - Transmit Interval seconds
cloud	n	pppwaitfor	1 - 255	WAN - Assume connection is lost after n timeouts
cloud	n	ethrxkeepalive	0 - 28800	Ethernet - Receive Interval seconds
cloud	n	ethtxkeepalive	0 - 28800	Ethernet - Transmit Interval seconds
cloud	n	ethwaitfor	1 - 255	Ethernet - Assume connection is lost after n timeouts

There is an additional cloud CLI command "**`cloudstat`**". Using this command with no extra syntax returns the status of the socket connections, i.e. whether there is a live connection to the device cloud server or not.

SNMP

Configuration – Remote Management > SNMP

The Simple Network Management Protocol (SNMP) is a well established way of managing clusters of remote routers – the TransPort routers support versions 1, 2c and 3 of this protocol. The standard Management Information Bases (MIBs) that are supported by the router are detailed below. Alongside these, there are two other MIBs that are supplied as standard. This is a MIB that is generated after the firmware has been installed. This is accomplished using the "mibprint" CLI command and the "MIBEXE" DOS tool which is available from the Technical Support Team. This MIB changes with every firmware release since the firmware revision is embedded in the Object Identifiers (OIDs). This MIB provides access to most of the configuration and statistics that are associated with the router.

The second MIB is the “Monitor MIB” which is a standard MIB that gives access to various Digi TransPort proprietary objects. The OIDs in this MIB do not change with every release although it is possible for new objects to be added to it. This MIB is available from the Technical Support team.

The standard MIBs supported are:

- SNMP MIB (RFC3418)
- Interfaces MIB (RFC2233)*
- IP MIB (RFC2011)
- IP Forwarding Table MIB (RFC2096)
- TCP MIB (RFC2012)
- UDP MIB (RFC2013)
- VRRP MIB (RFC2787)
- SNMP MPD MIB (RFC3412)
- SNMP USM MIB (RFC3414)**

* The following groups/tables in RFC2233 are not supported: ifXTable, ifStackTable, ifRcvAddressTable.

** The following groups/tables in RFC3414 are not supported: usmUserTable.

Other MIBs may be available on request.

Enable SNMPv1
Ticking this checkbox enables support for version 1 of the protocol.

Enable SNMPv2c
Ticking this checkbox enables support for version 2c of the protocol.

Enable SNMPv3
Ticking this checkbox enables support for version 3 of the protocol.

Use UDP Port n
This is the UDP port number to use. The default is UDP port 161.

SNMPv3 Engine ID
This is required as part of the SNMP v3 protocol. This is a 24 hexadecimal character string; any trailing zeroes in this string making the value up to 24 characters can be omitted. A remote engine ID is required when a SNMP v3 Inform is configured. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snmp	n	v1enable	0,1	Enable SNMPv1 0 = Off 1 = On
snmp	n	v2cenable	0,1	Enable SNMPv2c 0 = Off 1 = On
snmp	n	v3enable	0,1	Enable SNMPv3 0 = Off

Entity	Instance	Parameter	Values	Equivalent Web Parameter
				1 = On
snmp	n	port	0 - 65535	Use UDP Port Default = 161
snmp	n	engineid	String	SNMPv3 Engine ID

SNMP User > SNMP User n

Configuration – Remote Management > SNMP> SNMP User> SNMP User n

This page controls the configuration of the SNMP users.

SNMPv1 / SNMPv2c

Community
The text in this text entry box specifies the community string for Version 1 and Version 2c SNMP packets.

Confirm Community

The community string is echoed as dots in the text entry box and so having a second confirmation field where the string is retyped, allows a simple check to be performed for correct entry.

SNMPv3

Username
This field is the name of the SNMP user.

Authentication None, MD5, SHA1
These three radio buttons select what authentication algorithm is to be applied to the SNMP transactions.

Authentication Password
This is the authentication password for the user.

Confirm Authentication Password
The authentication password is not shown as clear text. The confirmation box allows a simple check that the password has been entered correctly.

Encryption None, DES, AES
These three radio buttons select which encryption (privacy) algorithm should be applied to the SNMP data.

Encryption Password
The user's password that is used to control the privacy of the SNMP transactions is entered into this text entry box.

Confirm Encryption Password
The encryption password is not shown as clear text. The confirmation box allows a simple check that the password has been entered correctly.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snmpuser	n	community	public / private	Community

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snmpuser	n	name	user_dave	Username
snmpuser	n	auth	Off,MD5,SHA1	Authentication, None, MD5, SHA1
snmpuser	n	authPassword	my_password	Authentication Password
snmpuser	n	priv	Off,DES,AES	Encryption, None, DES, AES
snmpuser	n	privPassword	my_password	Encryption Password

SNMP Filters

Configuration – Remote Management > SNMP> SNMP Filters

SNMP filters allow the system administrator to control access to the router MIBs via SNMP. This functionality is controlled by a table on the web configuration page. This table has three columns, two main headed columns as described below and a control column containing button widgets. The table has a capacity of ten entries, snmp filter instances range from 0 to 9.

Username
The username (as configured in the ***Configuration – Security > Users section***) of the user to whom the access restriction is applied.

OID Prefix
The Object ID prefix for the range of objects in the MIB that the user is not allowed to view. e.g. 1.3.6.1.2.1.4

Add
This button adds the username and OID prefix into the table.

Delete
This button causes the associated entry in the table to be deleted.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snmpfilter	n	user	username	Username
snmpfilter	n	oid	Valid SNMP OID	OID Prefix

SNMP Traps

Configuration – Remote Management > SNMP> SNMP Traps

SNMP traps are events that are generated when the specified condition is met. The web page and CLI configuration parameters are described here. The TansPort routers support two trap servers.

Generate Enterprise traps

When this check box is ticked, the router will generate product-specific traps.

Generate Generic traps

SNMP specifies several generic traps (Cold Start, Warm Start, Link Down, Link Up etc). When this checkbox is ticked, generic traps are generated.

Generate Authentication Failure traps
This checkbox enables the generation of authentication failure traps.

Generate VRRP traps
Checking this checkbox enables the generation of VRRP traps. See the VRRP section in this manual for the configuration of VRRP.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snmp	n	enterprisetraps	0,1	Generate Enterprise traps 0 = Off 1 = On
snmp	n	generictraps	0,1	Generate Generic traps 0 = Off 1 = On
snmp	n	authtraps	0,1	Generate Authentication traps 0 = Off 1 = On
snmp	n	vrrptraps	0,1	Generate VRRP traps 0 = Off 1 = On

SNMP Trap Server n

Configuration – Remote Management > SNMP> SNMP Traps > SNMP Trap Server n

Digi TransPort routers support two SNMP trap servers. The following options and description explain how to configure a trap server.

Trap Server IP Address a.b.c.d
This is the IP address of the server running the SNMP software and determines the destination for the trap notifications.

Port n
This is the UDP port number that the SNMP server is listening on, the default is 162 which is the standard port number for this service.

Use SNMP Version
Select the required SNMP version number from this drop-down selection box.

Send "Inform Request" message
If SNMP version 2c or 3 is selected, the router can send a SNMP Inform Request message instead of a Trap message. Inform Request messages are acknowledged by the SNMP Trap server whereas Trap messages are not.

If no response, retransmit the Inform Request message after n seconds
The period after which the Inform Request message is retransmitted if no response has been received.

Retransmit a maximum n times

The maximum number of times an Inform Request message will be retransmitted. If no acknowledgement is received after the maximum number of retransmissions, an event is logged.

Community
Enter the desired community string into this text entry box.

Confirm Community
Entering the community string again here enables verification of the string since the string is not displayed.

Trap Server Engine ID
This item will be configured within the application and is the SNMP server software engine ID which is used for authentication and encryption.

SNMP User
This is the username that should be associated with the trap server. This should match a user from one of the previously configured SNMP users (***Configuration – Remote Management > SNMP > Users***).

User Security Level
Select the desired security level from this drop-down selection box. The choices are these:
No Authentication, No Privacy
Authentication, No Privacy
Authentication, Privacy

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
snmptrap	n	IPaddr	Valid IP address e.g. 1.2.3.4	Trap Server IP Address a.b.c.d
snmptrap	n	port	0 - 65535	Port Default = 162
snmptrap	n	version	v1, v2c, v3	Use SNMP Version
snmptrap	n	sendInforms	on | off	Send “Inform Request” messages
snmptrap	n	informto	Integer	If no response, retransmit the Inform Request message after n seconds
snmptrap	n	informretries	Integer	Retransmit a maximum n times
snmptrap	n	community	String	Community
snmptrap	n	engineid	String	Trap Server Engine ID
snmptrap	n	securityname	String	SNMP User
snmptrap	n	securitylevel	noauthnopriv authnopriv authpriv	User Security Level noauthnopriv = No Authentication, No Privicy authnopriv = Auth, No Priv authpriv = Auth & Priv

Security Configuration

The ***Configuration – Security*** page has the following menu options:

- System
- Users
- Firewall
- RADIUS
- TACACS+
- Command Filters
- Calling Numbers
- GPS

Users

Configuration – Security> Users

The ***Configuration – Security> Users*** menu has the following sub-menu options:

- User n
- Advanced

User n

Configuration – Security> Users> User n

These pages allow you to configure a number of authorised users. The number of users available depends on the firmware build the router is running. Each user has a password and access level that determines what facilities the user has access to.

Username
The name of the user. Up to 14 characters are allowed.
There are some special usernames that can also be used, these are:
%s This uses the serial number of the router as the username.
%i This uses the IMEI of the cellular module as the username.
%c This uses the ICCID of the SIM as the username.

If a '%' symbol is part of the username, it must be escaped with another '%' symbol. For example 'user%1' should be entered as 'user%%1'.

Password / Confirm Password
The password for the user. Up to 14 characters are allowed.

Access Level
Selects the access level for the User. There are the following options

Super	Allows full access to all facilities.
High	Allows user to reconfigure the general configuration of the router and to change some settings such as the time and date. Not allowed to change user settings.
Medium	Allows user to access medium level configuration commands which allow some configuration of the router.

Low	Allows user to access low level commands which tend to be status and statistics commands.
Read Only	Read only access of the configuration.
None	User is not allowed to login via Web, FTP, SSH and Telnet.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
user	0	name	String (up to 14 chars)	Username
user	0	password	String (up to 14 chars)	Password
user	0	access	0 = Super 1 = High 2 = Medium 3 = Low 4 = None 8 = Read Only	Access Level

Advanced

Configuration – Security> Users> User n> Advanced

Allow this user to log in over a PPP network
Enabling this will allow the user to log in to the router using PPP. Disabling this will disable PPP login for the user no matter what the user's access level is.

Use this number x when PPP dial-back is required for this user
The telephone number for the user in the event that "dial-back" is required. If the username that the remote router uses during the PPP authentication matches the username of the user where a dial-back number is configured, the user's dial-back number will override any dial-back number configured in the answering PPP interface.

Alternate IKE Key / Confirm Alternate IKE Key
When IKE is the initiator, the responder supplied HASH is checked using the normal password (above) and if that fails, the Alternate Key (here). The initiator will remember which password was successful, and use that password to create the HASH if it becomes the responder of some new negotiation. If the IKE becomes a responder and IKE negotiations fail after supplying the HASH, the other password will be used during the next negotiation. Using this Alternate Key, it should be possible to configure new passwords into both ends of a tunnel, and not have too many failed negotiations. The process would be to add the Alternate Key into the remote router, then update the local router with the Alternate Key. Once that has been done, the administrator would then be able to move the Alternate Key to the usual location (Password) and remove the Alternate Key (newpwd) from the configuration. Should a negotiation take place during the period where the Alternate Key has been entered into the remote router, but not the local router, there should be no more than one failed negotiation, and only if the remote router is the initiator.

Remote Peer IP address
In certain circumstances, it may be desirable for a user connecting in over a PPP connection to be allocated a specific IP address, rather than be allocated an address from a pool

configured on a PPP interface. When this parameter is configured, the IP address negotiated on the PPP link will be this one, not an address from the regular IP address pool.

Remote Peer IP subnet
In the event that multiple PPP interfaces are enabled for answering and that multiple remote routers can dial into the local router, static routes cannot always be used to ensure that packets which should be routed to the remote network are sent through the correct PPP interface. This parameter can be used in conjunction with the 'Remote Peer IP subnet mask' parameter to associate a network subnet with a user.
When a remote unit "connects in" and authenticates with the unit, the unit will then create a dynamic route (that will override any static routes) for the duration of the PPP session. The interface for the dynamic route will be the PPP interface that answered the call. The network address for the dynamic route will be taken from the entry in the user table that matches the username that the remote unit used during the PPP authentication.

Remote Peer IP subnet mask
The remote subnet mask parameter is used in conjunction with the 'Remote Peer IP subnet' parameter above to fully qualify the network address for the user.

Public Key file
The name of the file containing the public key for that user. If the public key matches the client supplied public key, the user is allowed access.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
user	0	dun_en	on, off	Allow this user to log in over a PPP network
user	0	phonenum	Number	Use this number x when PPP dial-back is required for this user
user	0	newpwd	String (up to 14 chars)	Alternate IKE Key
user	0	fieldip	IP Address	Remote Peer IP address
user	0	ipaddr	IP Address	Remote Peer IP subnet
user	0	mask	IP Mask	Remote Peer IP subnet mask
user	0	keyfile	Filename	Public Key file

Firewall

Configuration – Security> Firewalls

All Digi TransPort routers incorporate a comprehensive firewall facility. A firewall is a security system that is used to restrict the type of traffic that the router will transmit or receive based on a combination of IP address, service type, protocol type, port number and IP flags. Firewalls are used to minimise the risk of unauthorised access to the local network resources by external users or to restrict the range of external resources to which local users have access. A more detailed description of how firewalls operate on Digi routers is given in the "Firewall Scripts" section. Refer to this section before attempting to implement a firewall.

The rules governing the operation of the firewall are contained in a pseudo-file called “fw.txt”. This file can be created either by using the controls in the web page described below or by using a text editor on a PC and then loading the resulting file onto the router using FTP or XMODEM. Digi Routers are shipped with a default fw.txt file that can be used as the starting point for a custom firewall configuration.

Configuration of the firewall is carried out by using the table described below. There are three other buttons that appear just below the table. Their use will also be described.

Since a default file is supplied, when this page loads it will show the rules in the default “fw.txt” file. If “fw.txt” does not exist, a blank table will be shown.

Hits
The numbers that appear in this column of the table are the number of hits for the rule that appears to the right.

#
This is non-editable and is simply the rule number.

Delete
Clicking this button deletes the rule that appears to its left.

Insert
These buttons are used to insert new lines. The insert buttons that appear alongside existing rules insert new blank lines above the line on which they appear. The button at the bottom creates a new blank line at the end of the table. (An empty table will only have the one button at the bottom). To create a new rule, click the button at the point the new rule should appear and a new text box should appear. Type the rule into the text box and once complete, click the “ok” button. To abandon any changes click the “cancel” button. Once the “ok” button has been clicked the firewall task will validate the rule and if valid, will add it the table. If errors are detected, a warning message will be displayed, at which point the rule may be edited or deleted.

Edit
These buttons that appear to the right of the rule open up the rule in an edit text box which allows the text to be edited. Click on the “ok” button to commit the changes or “cancel” to abandon the edit.

Reset Hit Counters
Clicking this button resets (to zero) all the rule hit counts that appear in the left-hand column of the table.

Save
Clicking this button saves changes to the table to the “fw.txt” file. If the changes are not saved using this button, they will be lost if the router is rebooted or loses power.

Restore
If, after reviewing changes to the table it is decided that the edit should be abandoned, clicking this button will restore the original “fw.txt” to the table, provided that they have not been saved.

Below the firewall editor table is another table that controls which interfaces the firewall rules apply to.

Interface
This column is simply a list of the available interfaces to which the firewall rules may be applied.

Enabled

Check the checkbox next to the interface(s) that the firewall should operate on in order to enable the firewall for that interface.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
fw	n/a	logclr	-	Reset Hit Counters
fw	n/a	save	-	Save
fw	n/a	-	-	Restore

The firewall rule hits may be viewed from the command line console by using the command:

type fwstat.hit

Stateful Inspection Settings

Configuration – Security> Firewalls> Stateful Inspection Settings

The page described below contains timer timeout values and other options that are used by the firewall stateful inspection module. This module establishes firewall rules that last for the duration of a single connection only. Typically, the first packet of a TCP connection (SYN packet) is used to create a stateful inspection rule that only allows subsequent packets for that TCP connection through the firewall. The timers described below are used to set limits on how long such rules persist.

Timers

TCP Opening s seconds
The value in this text box specifies the length of time following receipt of a TCP packet that causes a stateful inspection rule to be created before a TCP connection must be established. If a TCP connection is not established within this period, the associated stateful rule will be removed.

TCP Open s seconds
The value in this text box specifies the length of time that an established TCP connection may remain idle before the stateful inspection rule created for it is removed. The timer is restarted each time a packet is processed by the associated stateful inspection rule.

TCP Closing s seconds
The value in this text box specifies the length of time that is allowed for a TCP socket to close once the first FIN packet has been received. If the timer expires before the socket has completed closing, the stateful inspection rule is removed.

TCP Closed s seconds
The value in this text box specifies the length of time that a stateful inspection rule will remain in place after a TCP connection has closed.

UDP s seconds
The value in this text box specifies the length of time that a stateful inspection rule will remain in place following the receipt of UDP packet. The timer is restarted each time packets matching the rule pass in each direction. As a consequence, rules based on UDP should only be used if it anticipated that packets will travel in both directions.

ICMP s seconds
Some ICMP packets – for instance the ECHO request – generate response packets. The value in this text box specifies the length of time that a stateful inspection rule created for an ICMP packet will remain in place if the response is not received. The rule is removed immediately following receipt of the response.

Other protocols s seconds
If a stateful inspection rule is created from a packet type other than TCP, UDP or ICMP, a rule timeout should be created for it. The parameter in this text box specifies the length of time such a rule persists. The timer is restarted each time a packet is processed by the rule.

Other Options

Expire entry after n consecutive packets in one direction
The value in this text box specifies the maximum number of consecutive packets that should pass in one direction before the corresponding rule entry is expired.

Count missed UDP echo packets as dropped
When checked, this checkbox will cause the firewall to increment the dropped packet count for each failed echo request in the situation where UDP echo is active on an interface that becomes disconnected.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
fwall	0	opening	0 - 4294967296	TCP Opening s seconds
fwall	0	open	0 – 4294967296	TCP Open s seconds
fwall	0	closing	0 - 4294967296	TCP Closing s seconds
fwall	0	closed	0 – 4294967296	TCP Closed s seconds
fwall	0	udp	0 – 4294967296	UDP s seconds
fwall	0	icmp	0 – 4294967296	ICMP s seconds
fwall	0	other	0 – 4294967296	Other protocols s seconds
fwall	0	maxuni	0 - 2147483647	Expire entry after n consecutive packets in one direction
fwall	0	cntmissedecho	OFF,ON Default OFF	Count missed UDP echo packets as dropped

RADIUS

Configuration – Security> Radius

The RADIUS client may be used for authentication purposes at the start of remote command sessions, SSH sessions, FTP sessions, HTTP sessions and Wi-Fi client connections (PEAP & EAP-TLS). Depending on how the RADIUS client is configured, the router may authenticate with one or two RADIUS servers, or may authenticate a user locally using the existing table configured on the router.

There are 2 RADIUS client configurations, RADIUS client 0 and RADIUS client 1, both have specific functions and the correct instance (0 or 1 or both) should be configured depending on the requirements.

To use RADUIUS for authenticating router administration access, configure RADIUS client 0. To use RADUIUS for authenticating Wi-Fi clients, configure RADIUS client 1.

When the router has obtained the remote user username and password, the RADIUS client is used to pass this information (from the Username and Password attributes) to the specified RADIUS server for authorisation. The server should reply with an ACCEPT or REJECT message.

The RADIUS client may be configured with up to two Network Access Servers (NAS). It may also have local authentication turned on or off depending on system requirements.

When a user is authenticated, the configured RADIUS servers are contacted first. If a valid ACCEPT or REJECT message is received from the server, the user is allowed or denied access respectively. If no response is received from the first server, the second server is tried (if configured). If that server fails to respond, local authentication is used unless disabled. If both servers are unreachable and local authentication is disabled, all authentication attempts fail.

If a RADIUS server replies with a REPLY-MESSAGE attribute (18), the message will be displayed to the user after the login attempt and after any configured “post-banner” message. The router will then display a “Continue Y/N?” prompt to the user. If “N” is selected, the remote session will be terminated. This applies to remote command sessions and SSH sessions only.

If the login attempt is successful and the server sends an IDLE-TIMEOUT attribute (28), the idle time specified will be assigned to the remote session. If no IDLE-TIMEOUT attribute is sent, the router will apply the default idle timeout values to the session.

The access level is determined by the value of the SERVICE-TYPE attribute returned by the RADIUS server. Administrative access is determined by the value 6 being returned by the server. Any other value or no value returned will result in the access level “low” being assigned.

When the session starts and ends, the router will send the RADIUS accounting START/STOP messages to the configured server. Again, if no response is received from the primary accounting server, the secondary server will be tried. No further action is taken if the secondary accounting server is unreachable.

As a consequence of the fact that the router has separate configurations for authorisation and accounting servers, it is possible to configure the router to perform authorisation functions only, accounting only, or both. An example of how this might be used could be to perform local authorisations but send accounting start/stop records to an accounting server.

RADIUS Client n

Configuration – Security> Radius > RADIUS Client n

The following pages describe the configuration parameters available for setting up a RADIUS client on the router.

Authorization

Primary Authorization Server

IP Address a.b.c.d
The value in this text box specifies the IP address of the primary authorisation NAS.

NAS ID
The value in this text box is an identifier which is passed to the primary authorisation NAS and is used to identify the RADIUS client. The appropriate value will be supplied by the primary authorisation NAS administrator.

Password
The value in this text box is the password supplied by the primary authorisation NAS administrator and is used in conjunction with the primary authorisation NAS ID to authenticate RADIUS packets.

Confirm Password
Type the above password into this text box so that the router may determine if the two are identical.

Secondary Authorization Server

IP Address a.b.c.d
The value in this text box is the IP address of the secondary authorisation NAS server.

NAS ID
The value in this text box is an identifier which is passed to the secondary authorisation NAS and is used to identify the RADIUS client. The appropriate value will be supplied by the secondary authorisation NAS administrator.

Password
The value in this text box is the password supplied by the secondary authorisation NAS administrator and is used in conjunction with the secondary authorisation NAS ID to authenticate RADIUS packets.

Confirm Password
Type the above password into this text box so that the router may determine if the two are identical.

Enable local authorization if there is no response from the authorization server(s)
When checked (default state), this checkbox will allow local authorisation if the RADIUS servers are unreachable or not configured. Uncheck the box to disable local authorisation.

Accounting

Primary Accounting Server

IP Address
The value in this text box is the IP address of the primary accounting NAS.

NAS ID
The value in this text box is an identifier that is passed to the primary accounting NAS and is used to identify the RADIUS client. The appropriate value will be supplied by the primary accounting NAS administrator.

Password
The value in this text box is the password that is supplied by the primary accounting NAS administrator and is used in conjunction with the primary accounting NAS ID to authenticate RADIUS packets.

Confirm Password
Type the above password into this text box to enable the router to check that they are identical.

Secondary Accounting Server

IP Address
The value in this text box is the IP address of the secondary accounting NAS.

NAS ID
The value in this text box is an identifier that is passed to the secondary accounting NAS and is used to identify the RADIUS client. The appropriate value will be supplied by the secondary accounting NAS administrator.

Password

The value in this text box is the password that is supplied by the secondary accounting NAS administrator and is used in conjunction with the secondary accounting NAS ID to authenticate RADIUS packets.

Confirm Password
Type the above password into this text box to enable the router to check that they are identical.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
radcli	0,1	server	Valid IP Address a.b.c.d	Primary Authorization Server IP Address
radcli	0,1	nasid	Up to 80 characters	Primary Authorization Server NAS ID
radcli	0,1	password	Up to 40 characters	Primary Authorization Server Password
radcli	0,1	server2	Valid IP Address a.b.c.d	Secondary Authorization Server IP Address
radcli	0,1	nasid2	Up to 80 characters	Secondary Authorization Server NAS ID
radcli	0,1	password2	Up to 40 characters	Secondary Authorization Server Password
radcli	0,1	localauth	OFF,ON Default ON	Enable local authorization if there is no response from the authorization server(s)
radcli	0,1	aserver	Valid IP Address a.b.c.d	Primary Accounting Server IP Address
radcli	0,1	anasid	Up to 80 characters	Primary Accounting Server NAS ID
radcli	0,1	apassword	Up to 40 characters	Primary Accounting Server Password
radcli	0,1	aserver2	Valid IP Address a.b.c.d	Secondary Accounting Server IP Address
radcli	0,1	anasid2	Up to 80 characters	Secondary Accounting Server NAS ID
radcli	0,1	apassword2	Up to 40 characters	Secondary Accounting Server Password

Advanced

Configuration – Security> Radius> Radius Client n> Advanced

If there is no response from the server

Use Source IP Address

If required an alternative source interface and instance may be selected here. Select the required interface from the drop-down list and enter the instance of that interface into the adjacent text box. The available interface options are

- **Auto**
- **PPP**
- **Ethernet**

Retransmit the request after s seconds
The value in this text box specifies the interval between retransmissions of RADIUS packets.

Stop the negotiation after n retransmissions
The value in this text box specifies the maximum number of times RADIUS data should be transmitted to the NAS before the negotiation is deemed to have failed.

Stop the negotiation if there is no activity for s seconds
The value in this text box specifies the inactivity period after which the negotiation procedure is deemed to have failed.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
radcli	0	ip_ent	Blank,ETH,PPP Blank = Auto	Use Source IP Address
radcli	0,1	retranint	0 – 2147483647 Default 5	Retransmit the request after s seconds
radcli	0,1	retran	0 – 2147483647 Default 3	Stop the negotiation after n retransmissions
radcli	0,1	inactto	0 – 2147483647 Default 30	Stop the negotiation if there is no activity for s seconds

TACACS+

Configuration – Security> TACACS+

The Digi TransPort range of routers supports Terminal Access Controller Access-Control System Plus (TACACS+) for controlling access to the router. TACACS+ provides authentication, authorisation and accounting (AAA) services.

TACACS+ can be used to control the following access methods: Secured asynchronous serial (ASY) ports, Telnet, SSH, FTP, HTTP/HTTPS and SNMP.

When any sort of request is to be performed by the TACACS+ client, the client first checks to see if a socket to the server (primary or backup) is already open. If a socket is already open, that socket is used for the TACACS+ request. If no socket is open, the primary server is tried first. If the primary server socket fails to open, the backup server will be tried. Regardless of whether the primary or backup socket connected, the primary server is always tried first on the next connection attempt. Once the connection to the TACACS+ server opens, all pending requests are sent to the TACACS+ server.

If a connection to the TACACS+ server is not possible due to network or server problems, all requests by applications are denied.

Functions of the AAA services

If TACACS+ authentication is enabled, the request is sent to the TACACS+ server. If disabled, the router performs the authentication. At this point authorisation is also performed. If TACACS+ authorisation is disabled, the user access level is obtained from the local user table on the router. If TACACS+ authorisation is enabled, an authorisation request is sent to the TACACS+ server. The server will return a privilege level and may also return other attributed such as a new idle time for this session which takes precedence over locally configured values.

When the user has been authenticated and access has been authorised, the login is allowed. If the connection is via telnet or SSH a welcome message will be displayed that shows the access level and the method of authentication. If the access level was assigned locally the following message will be displayed:

Welcome. Your access level is SUPER

If the access level was assigned by the TACACS+ server, the following message will be displayed:

Welcome. Your access level is obtained remotely

If accounting is enabled, session start and stop messages are sent to the TACACS+ server when the session opens and closes. During the session, details of commands executed and denied due to access level control will be sent to the TACACS+ server. At the end of the session the stop message is sent to the TACACS+ server with the elapsed session time included.

TACACS+ to local privilege level mappings:

TACACS+ level	Local level
>= 15	Super
12 - 14	High
8 – 11	Medium
4 - 8	Low
0 - 3	None

Primary TACACS+ Server

Hostname or IP address of Server a.b.c.d Port n
The IP address or hostname of the primary TACACS+ server is entered into the left-hand text box. If required a port number may also be specified using the right-hand text box. TACACS+ uses TCP port 49 by default. Entering a different number into this text box will cause the router to use that port instead. The port number is used by both the primary and secondary TACACS+ servers.

Server Key
The value in this text box specifies the encryption key to use when communicating with the primary server.

Confirm Server Key
The key is typed into this text box to allow the router to confirm that the two strings are identical.

Secondary TACACS+ Server

Hostname or IP address of Server
The value in this text box is the IP address or hostname of the secondary (backup) TACACS+ server. This will be used if a socket to the primary server cannot be opened.

Server Key
The value in this text box is the encryption key to use when communicating with the secondary server.

Confirm Server Key
Enter the key into this text box to allow the router to confirm that the two entries are identical.

Enable local authentication if there is no response from the server(s)
When checked, this checkbox will allow local authentication if TACACS+ authentication fails.

Enable TACACS+ Authentication
When checked, this checkbox enables authentication. When authentication is enabled, user authentication takes place on the TACACS+ server. When disabled, user authentication takes place locally on the router.

Enable TACACS+ Authorisation
When checked, this checkbox enables authorisation which means that authorisation of the application takes place and authorisation of application-related commands also takes place.

Enable TACACS+ Accounting
When checked, this checkbox enables accounting. When accounting is enabled, accounting messages are sent at the start and end of application sessions (where applicable) and update messages are also sent from command sessions when commands are denied locally or after they are executed.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
tacplus	0	svr	Up to 64 characters for hostname or valid IP address a.b.c.d	Hostname or IP address of server
tacplus	0	port	0 – 2147483647 Default 49	Port
tacplus	0	key	Up to 20 characters	Server Key
tacplus	0	svr2	Up to 64 characters or valid IP address a.b.c.d	Hostname or IP address of server
tacplus	0	key2	Up to 20 characters	Server Key
tacplus	0	localauth	OFF,ON	Enable local authentication if there is no response from the server(s)
tacplus	0	authent	OFF,ON	Enable TACACS+ Authentication
tacplus	0	author	OFF,ON	Enable TACACS+ Authorisation
tacplus	0	acct	OFF,ON	Enable TACACS+ Accounting
tacplus	0	debug	OFF,ON	n/a
tacplus	0	tacacspageauth	OFF,ON	n/a

Advanced

Configuration – Security> TACACS+> Advanced

The parameters described in this section should not normally need to be adjusted.

Use source IP Address x,y

If required, due to the TACACS+ server being accessed via a VPN tunnel, an alternative source interface and instance may be selected here. Select the required interface from the drop-down list and enter the instance of that interface into the adjacent text box. The available interface options are

- **Auto**
- **PPP**
- **Ethernet**.

Response Timeout s seconds
Text box

Stop the negotiation if there is no activity for s seconds
The number in this text box specifies the amount of time (in seconds) before an inactive socket is closed.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
tacplus	0	ip_ent	Blank,ETH,PPP Blank = Auto	Use source IP Address x,y
tacplus	0	ip_add	0 - 2147483647	Use source IP Address x,y
tacplus	0	respto	0 – 2147483647 Default = 30	Response Timeout s seconds
tacplus	0	inact	0 – 2147483647 Default = 30	Stop the negotiation if there is no activity for s seconds

Command Filters

Configuration – Security> Command Filters

When this feature is enabled, commands will not reach the router's command interpreter unless they are defined in the Command Filters table. Terminal devices may send commands that the router will not necessarily understand but that require a basic "OK" or "ERROR" response.

With command filtering turned on, any command entered will be responded to with a MODEM-like "OK" or "ERROR" response (depending on settings below) unless the command is found in the Command Filters table. The command filter uses wild-character matching so that command filters such as "cmd*" are permitted which would allow all "cmd 0 ..." commands to be executed. Note that the command mapping table is checked first and the command filter table is only checked if there was not a match in the command matching table.

For more information on command filtering there is an application note "Command Line Response Manipulation" which is available on the Digi web site (***www.digi.com***).

The table is generated by typing the desired command into the text box and clicking the "Add" button. Once a command has been entered into the table, it can be removed by clicking the "Delete" button that appears on the right hand side.

Command
This text box contains the command to filter.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter

Entity	Instance	Parameter	Values	Equivalent Web Parameter
cfilter	n	cmd	Valid command line command	Command
cmd	n	cfilton	0,1 0 = Off 1 = On	n/a
cmd	n	cfilterr	0,1 0 = Off – OK 1 = On – ERROR	n/a

Command filtering is enabled from the command line for any particular instance of the command interpreter with the following command **`cmd <n> cfilton 1`**

The default action is to respond with the "OK" response. If the response needed is "ERROR", use the parameter **`cmd <n> cfilterr 1`**

Where n is the instance number.

Note:
If the command string contains blank characters, it must be enclosed by double quotation marks. When substituting a command, upper case characters are considered the same as the corresponding lower case characters.

Calling Numbers

Configuration – Security> Calling Numbers

Note:
This feature is for use by experienced personnel for network testing and fault diagnosis. It should not be required for normal use. To use this feature, the ISDN circuit must support the Calling Line Identification (CLI) facility. If CLI is supported, incoming calls from specified numbers may be answered normally or alternatively rejected with an optional reject code.

This web page contains a table that accepts a series of telephone numbers, each of which has an associated Answer or Reject parameter and in the case of numbers from which calls are to be rejected, a user-defined reason code. For each number set to "Reject", the router will reject incoming calls from that number using the reason code specified. The reason code is simply a numeric value that is chosen to suit the particular application. If any one of the entries is set to "Answer" the router will only answer incoming calls from that number and will reject calls from other numbers using a standard ISDN reject code.

Number
The number in this text box is the telephone number to either answer or reject.

Mode
The drop-down list in this column selects either "Answer" to answer calls or "Reject" to reject calls.

Reject Code
The value in this text box is the reason code pertaining to the rejection of the call.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
rejlst	n	num	up to 20 digits	Number

Entity	Instance	Parameter	Values	Equivalent Web Parameter
rejlst	n	ans	OFF,ON	Mode Answer,Reject
rejlst	n	code	0 – 255	code

Command line examples:

To display an entry in the calling numbers list enter the command:

rejlst <instance> ?

where *<instance>* is 0 – 9.

e.g. *rejlst 5 ?*

To set up an entry to reject a number, use the following commands:

rejlst 0 num 1234567

rejlst 0 ans OFF

rejlst 0 code 42

To set up an entry to answer a number, use the following commands:

rejlst 1 num 1234567

rejlst 1 ans ON

Position Configuration

The ***Configuration – Position*** page has ***GPS*** sub-menu item.

GPS

Configuration – Position > GPS

One of the options available on some models is the ability to connect a GPS receiver which enables the router access to geographical position information. The module may be internal or external. In either situation, an internal asynchronous serial (ASY) port will be used for the connection. The standard way that GPS modules send the data is using National Marine Electronics Association (NMEA) standard 0183 messages. This protocol is usually simply referred to as NMEA. Routers offering this functionality support the most common NMEA data messages. These will be described below. GPS receiver modules normally accept configuration commands which specify which of the NMEA messages should be sent to the requesting host. The following descriptions show how to configure a router to accept and forward GPS data using the web interface and by using CLI commands.

Enable local monitoring
When checked, this checkbox allows messages from the GPS receiver may be viewed on the ***Management – Position > GPS*** status page. Which messages are displayed is configured via entries in a table.

GPS Module Initialization String
Some GPS receivers may require configuration via an initialization message at start-up in order to send the appropriate messages in the required format, at the required data rate. Any such required command string is entered into the text entry box and will be sent to the attached GPS receiver module when the router initialises the module.
The table described here controls which NMEA messages should be sent from the module. The default is to enable all messages.

Fix data (GGA)
When the associated checkbox is checked the fix data (2D, 3D or no fix) will be output.

Position (GLL)
This checkbox, when checked, causes the Geographic position (Latitude/Longitude) sentence to be output.

Active Satellites (GSA)
Checking this checkbox causes the NMEA sentence containing the number of active satellites used to calculate the position, to be output.

Satellites in view (GSV)
Checking this checkbox causes the NMEA sentence containing the number of satellites in view to be output.

Position and Time (RMC)
Checking this checkbox causes the NMEA sentence containing the current position and time, to be output.

Course over Ground (VTG)
Checking this checkbox causes the NMEA sentence containing the course data to be output.

UTC and local date/time data (ZDA)
Checking this checkbox causes the NMEA sentence containing the current local time and date, to be output.

All other messages
The above messages are the most common and useful NMEA sentences. Many GPS modules support additional messages. Checking this checkbox causes the modules to output any other supported messages.

IP Connection 1

GPS data may be sent to up to two IP destinations. These are specified in the following two sections of the web page.

Send GPS messages to IP address a.b.c.d
This text entry box holds the IP address that the GPS data should be sent to.

Port n
The required TCP/UDP port number that the GPS data should be sent to is specified here.

Every n interval(s)
The number entered into this text entry box controls how often the GPS data is transmitted to the specified host. A value of 1 will cause collected GPS data to be transmitted each time a UTC and local date/time data (ZDA) message is received from the GPS receiver module. A value of 2 will cause every second message to be sent and so on. For this feature to work over a TCP/IP connection, the ZDA message must be enabled.

Use TCP / UDP
These radio buttons select which protocol to use for sending the messages.

Prefix the message with t
Enter any text string that the user wishes to precede the NMEA data into this text entry box.

Suffix the message with t
Enter any text string that the user wishes to follow the NMEA data into this text entry box.

IP Connection 2

Send GPS messages to IP address a.b.c.d
This text entry box holds the IP address that the GPS data should be sent to.

Port n
The required TCP/UDP port number that the GPS data should be sent to is specified here.

Every n interval(s)
The number entered into this text entry box controls how often the GPS data is transmitted to the specified host. A value of 1 will cause collected GPS data to be transmitted each time a UTC and local date/time data (ZDA) message is received from the GPS receiver module. A value of 2 will cause every second message to be sent and so on. For this feature to work over a TCP/IP connection, the ZDA message must be enabled.

Use TCP / UDP
These radio buttons select which protocol to use for sending the messages.

Prefix the message with t
Enter any text string that the user wishes to precede the NMEA data into this text entry box.

Suffix the message with t
Enter any text string that the user wishes to follow the NMEA data into this text entry box.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
gps	0	asy_add	The ASY port the GPS receiver is	n/a

Entity	Instance	Parameter	Values	Equivalent Web Parameter
			connected to	
gps	0	gpson	On, Off	Enable local monitoring
gps	0	init_str	Valid command for GPS receiver	GPS Module Initialization string
gps	0	gga_on	0,1 0 = Off 1 = On	Fix data (GGA)
gps	0	gll_on	0,1 0 = Off 1 = On	Position (GLL)
gps	0	gsa_on	0,1 0 = Off 1 = On	Active Satellites (GSA)
gps	0	gsv_on	0,1 0 = Off 1 = On	Satellites in view (GSV)
gps	0	rmc_on	0,1 0 = Off 1 = On	Position and time (RMC)
gps	0	vtg_on	0,1 0 = Off 1 = On	Course over Ground (VTG)
gps	0	zda_on	0,1 0 = Off 1 = On	UTC and local date/time (ZDA)
gps	0	oth_on	0,1 0 = Off 1 = On	All other messages
gps	0	IPaddr1	Valid IP address a.b.c.d	Send GPS message to IP address (1)
gps	0	IPport1	Valid IP port n	port n
gps	0	nsecs1	Time s seconds	every n interval(s)
gps	0	udpmode1	0,1 0 = TCP 1 = UDP	Use TCP/UDP
gps	0	IPprefix1	Free text	Prefix the message with
gps	0	IPsuffix1	Free text	Suffix the message with
gps	0	IPaddr2	Valid IP address a.b.c.d	Send GPS message to IP address (2)
gps	0	IPport2	Valid IP port n	port n
gps	0	nsecs2	Time s seconds	every n interval(s)

Entity	Instance	Parameter	Values	Equivalent Web Parameter
gps	0	udpmode2	0,1 0 = TCP 1 = UDP	Use TCP/UDP
gps	0	IPprefix2	Free text	Prefix the message with
gps	0	IPsuffix2	Free text	Suffix the message with

The following CLI parameters are not available on the web interface:

Entity	Instance	Parameter	Values	Equivalent Web Parameter
gps	0	gga_int	s seconds 0 – 255	n/a
gps	0	gll_int	s seconds 0 - 255	n/a
gps	0	gsa_int	s seconds 0 – 255	n/a
gps	0	gsv_int	s seconds 0 – 255	n/a
gps	0	rmc_int	s seconds 0 – 255	n/a
gps	0	vtg_int	s seconds 0 – 255	n/a
gps	0	zda_int	s seconds 0 - 255	n/a

Additional GPS CLI commands

cmd <instance> gpson {on|off}

When set to on, this indicates that an instance of the command line interpreter is connected to the GPS receiver. The instance number should be the ASY port number to which the GPS receiver is connected. This parameter has two purposes. Firstly, it tells a particular command interpreter instance that it is connected to a GPS receiver so that commands received by that instance should be ignored, rather than being treated as invalid commands. Secondly, it is used by the *at\gps* command to determine where the GPS messages originate.

at\gps

This command causes messages from the GPS receiver to be sent directly to the ASY port from which the command has been entered. This requires that the *gpson* parameter (above) is set to “on” for one of the command interpreter instances. As soon as the *at\gps* command has been issued, data from the GPS receiver will be sent to that ASY port. In order to stop the GPS data, the “+++” escape sequence must be entered, followed by a pause, followed by “*at*”.

Applications Page

The ***Configuration – Application*** page has the following menu options:

- Basic
- Python

Basic Applications

Configuration – Application > Basic

ScriptBasic

Configuration – Application > Basic > ScriptBasic

In order to allow end users to extend and enhance the functionality of the TransPort routers, scripting support is provided. ScriptBasic is a scripting language supported by Digi TransPort routers. This section describes how to run simple ScriptBasic scripts. The main configuration entity is a table containing a list of reference numbers and associated user parameters. The second is a text box containing the name of the script to run. Initially, the table is displayed empty, with a row that states "No parameters have been defined". The leftmost column contains the number "1".

n
This is the number of the parameter that appears in the next column. Up to 30 parameters may be configured. It is best to enter the numbers in a consecutive, ascending sequence since this is how the parameters will be referred to in any ScriptBasic script.

Parameter
Type the name of the parameter you wish to create. This can be any alphanumeric string. These parameters can then be referenced by a ScriptBasic script. For example, a script using parameter "string1" will use the string defined in the text entry box associated with command index 1.

Add
Clicking this button adds the parameter to the list of parameters. Parameters are added consecutively, with each parameter number referring to the string in the adjacent column.

Run Script
The text in this text entry box is the name of the ScriptBasic file to run. This script must exist within the filing system. Conventionally, ScriptBasic scripts use the ".sb" file extension, e.g."myscript.sb".

Run
Clicking this button will cause the ScriptBasic interpreter to run the named script.

Stop
Clicking this button will stop the execution of the ScriptBasic script.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
basic	0	string1 – string30	Free form alphanumeric text	Parameter
basic	0	n/a	kill	Stop
bas	n/a	n/a	Name of	Run Script

Entity	Instance	Parameter	Values	Equivalent Web Parameter
			ScriptBasic script	

Examples

To set User parameter 1 to IPv4 address 10.1.1.1, enter the command:

basic 0 string1 10.1.1.1

To execute a script from the CLI, enter the command:

bas <myscript.sb>

To kill a running script from the CLI, enter the command:

Basic 0 kill

Python Applications

Configuration – Application > Python

Python Files

Configuration – Application > Python > Python Files

Some of the Digi TransPort routers support the Python scripting language which gives users the facility to extend and enhance the basic functionality of the router. The routers contain a Python interpreter which may be invoked from the command line. This can be useful for developing scripts. The more usual way to use Python is to write a script to implement a required function and to run this script autonomously. It is common practice for python scripts to use the file extension ".py", e.g. "myscript.py". A Python script is a text file containing python commands and may be created using a normal plain text editor. Python is a powerful language and obtains some of its power from the many modules that are available for it. A description of the Python language is outside the scope of this manual.

Module search path
The parameter in this text entry box sets the search path for Python modules that are not in the default search path. Multiple locations may be specified by separating pathnames with colons, e.g. "pymod1.zip:python21.zip". This will cause the interpreter to search for the two compressed files pymod1.zip and python21.zip. Note that TransPort routers have a flat filing system structure that does not support subdirectories.

Redirect the Python output to debug
When checked, this checkbox allows the redirection of the stdout file handle to the debug output (stderr) file handle. The default state of this parameter is "Off". The easiest way to see this in action is to issue the command to start the Python interpreter from a debug/CLI terminal and note that the screen remains blank. Stop the interpreter (using the "exit()" command), set this parameter to "ON" and re-issue the command to start the interpreter. This time, the familiar Python welcome message and prompt should appear on the console.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
pycfg	0	modpath	valid search path, e.g. "mymod.py"	Module search path
pycfg	0	stderr2stdout	0,1 0 = Off 1 = On	Redirect the Python output to debug

The following additional command line informational / debugging commands may be helpful when developing Python scripts.

“*pycfg files*” which displays the status of any Python files.

“*pycfg mem*” which shows the memory useage for the router.

“*pycfg scripts*” which shows the status of any scripts and change count.

Management Page

The ***Management*** page has the following webpage options:

- Network Configuration
- Connections
- Position
- Analyser
- Top Talkers

Network Status Management

The ***Management-Network Status*** webpage has the following menu options:

- Interfaces
- IP Statistics
- IP Routing Table
- IP Hash Table
- Port Forwarding Table
- Firewall
- Firewall Trace
- DHCP Status
- DNS Status
- QoS

Interfaces

Management-Network Status> Interfaces

The ***Management-Network Status> Interfaces*** menu has the following sub-menu options:

- Ethernet
- Wi-Fi
- Mobile
- DSL
- GRE
- ISDN
- Serial
- Advanced

Ethernet >ETH n

Management-Network Status> Interfaces > Ethernet > Eth n

This page displays the current status and statistics of the selected Ethernet interface.

IP Address
The IP address of the Ethernet interface. This could be either manually configured or assigned via DHCP.

Mask
The mask of the Ethernet interface. This could be either manually configured or assigned via DHCP.

DNS Server / Secondary DNS Server
The primary and secondary DNS Server IP addresses of the Ethernet interface. These could be either manually configured or assigned via DHCP.

Gateway
The IP gateway of the Ethernet interface. This could be either manually configured or assigned via DHCP.

MAC Address
The Ethernet interface's MAC address.

Speed
The current speed of the Ethernet interface.

Duplex
The current duplex mode of the Ethernet interface.

Bytes Received
The number of bytes that have been received on the Ethernet interface.

Bytes Sent
The number of bytes that have been sent on the Ethernet interface.

Packets Received
The number of packets that have been received on the Ethernet interface.

Packets Sent
The number of packets that have been sent on the Ethernet interface.

Unicast Packets Received
The number of unicast packets that have been received on the Ethernet interface.

Unicast Packets Sent
The number of unicast packets that have been sent on the Ethernet interface.

Broadcast Packets Received
The number of broadcast packets that have been received on the Ethernet interface.

Broadcast Packets Sent
The number of broadcast packets that have been sent on the Ethernet interface.

Multicast Packets Received
The number of multicast packets that have been received on the Ethernet interface.

Multicast Packets Sent
The number of multicast packets that have been sent on the Ethernet interface.

Rx Overruns
The number of receive overruns that have occurred on the Ethernet interface. An Rx overrun occurs when there are not enough buffers to receive incoming packets which results in the received packets being dropped.

Collisions
The number of times the router has detected a packet collision on the Ethernet network when transmitting a packet.

Late Collisions
The number of times the router has detected a late packet collision on the Ethernet network when transmitting a packet.

Flood Protection
The number of times the router has detected an Ethernet packet flood on the network and has enabled the Flood Protection mechanism. Flood protection is designed to stop the router from being overwhelmed by the sudden large increase in packets on the Ethernet network.

Alignment Errors
The number of alignment errors that have been detected when receiving an Ethernet packet.

FCS Errors

The number of Ethernet packets that have been received but had an invalid FCS.

Tx Deferred
The Ethernet packets successfully transmitted after being initially deferred.

Long Frames
The number of Ethernet packets that have been received which are too long.

Carrier Sense Error
The number of carrier sense errors that have occurred. These occur when the router attempts to transmit an Ethernet packet but cannot detect the carrier sense condition on the Ethernet network.

Rx MAC Errors
The number of internal errors that have occurred when receiving an Ethernet packet.

Tx MAC Errors
The number of internal errors that have occurred when attempting to transmit an Ethernet packet.

Other Errors
The number of errors that have occurred which are not counted by the other statistics.

Related CLI Commands

Command	Instance	Parameter	Equivalent Web Parameter
eth	n	status	Displays the current configuration and status of Ethernet interface n.
ethstat	n	n/a	Displays the statistics for Ethernet interface n.
at\mibclr=eth.n.stats	n/a	n/a	Clears the statistics for Ethernet interface n.

Wi-Fi

Management-Network Status> Interfaces > Wi-Fi

Module Detected
This indicates that the Wi-Fi hardware has been detected by the router.

Admin Status
The current administrative state of the Wi-Fi interface. It indicates whether there is sufficient configuration to bring the Wi-Fi interface up. It can be either “Up” or “Down”.

Operational Status
The current operational state of the Wi-Fi interface. It can be either “Up” or “Down”.

Channel Mode
The Wi-Fi channel mode that is being used. The possible values for this parameter are “B/G” and “A”.

Channel
The Wi-Fi channel that is being used.

Bytes Received
The number of bytes that have been received on the Wi-Fi interface.

Bytes Sent
The number of bytes that have been sent on the Wi-Fi interface.

Packets Received
The number of packets that have been received on the Wi-Fi interface.

Packets Sent
The number of packets that have been sent on the Wi-Fi interface.

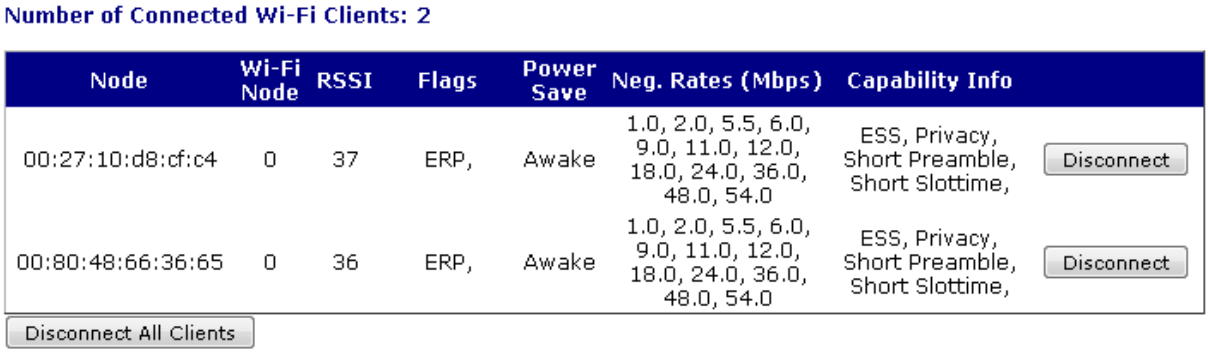
Receive Errors
The number of receives errors have occurred on the Wi-Fi interface.

Transmit Errors
The number of transmit errors have occurred on the Wi-Fi interface.

Received Packets Dropped
The number of received packets have been dropped on the Wi-Fi interface.

Wi-Fi Client Connections Table

This table gives information on the Wi-Fi clients that are connected to the router's Wi-Fi Access Point interface.



Node
The MAC address of the connected Wi-Fi client.

Wi-Fi Node
The Wi-Fi node on the router the client is connected to.

RSSI
The signal strength experienced by the Wi-Fi client.

Flags
The state information for the Wi-Fi client connection.

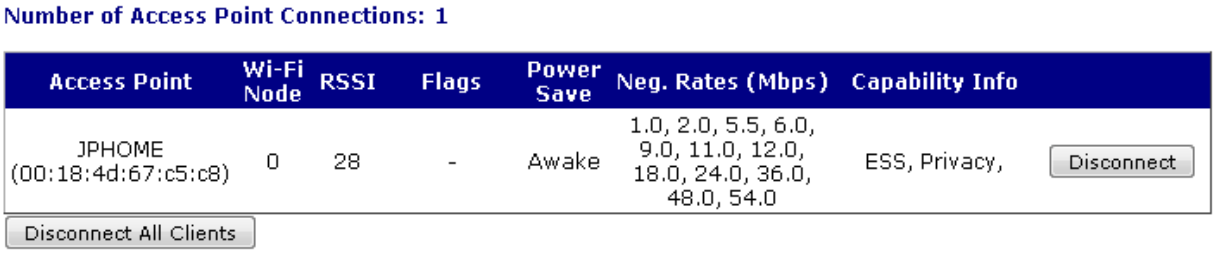
Power Save
The current power saving state of the Wi-Fi client. The possible values are "Awake" and "Sleep".

Neg. Rates (Mbps)
The transmission rates that have been negotiated with the Wi-Fi client.

Capability Info
The capabilities that the router has advertised to the Wi-Fi client.

Access Point Connections Table

This table gives information on the Wi-Fi Access Points that the router is connected to.



Access Point
The name and MAC address of the Wi-Fi Access Point that the router is connected to.

Wi-Fi Node
The Wi-Fi node that has been used to connect to the Access Point.

RSSI
The signal strength experienced by the router when connected to the Wi-Fi Access Point.

Flags
The state information for the Wi-Fi Access Point connection.

Power Save
The current power saving state of the router. The possible values are “Awake” and “Sleep”.

Neg. Rates (Mbps)
The transmission rates that have been negotiated with the Wi-Fi Access Point.

Capability Info
The capabilities of the Access Point that the router is connected to.

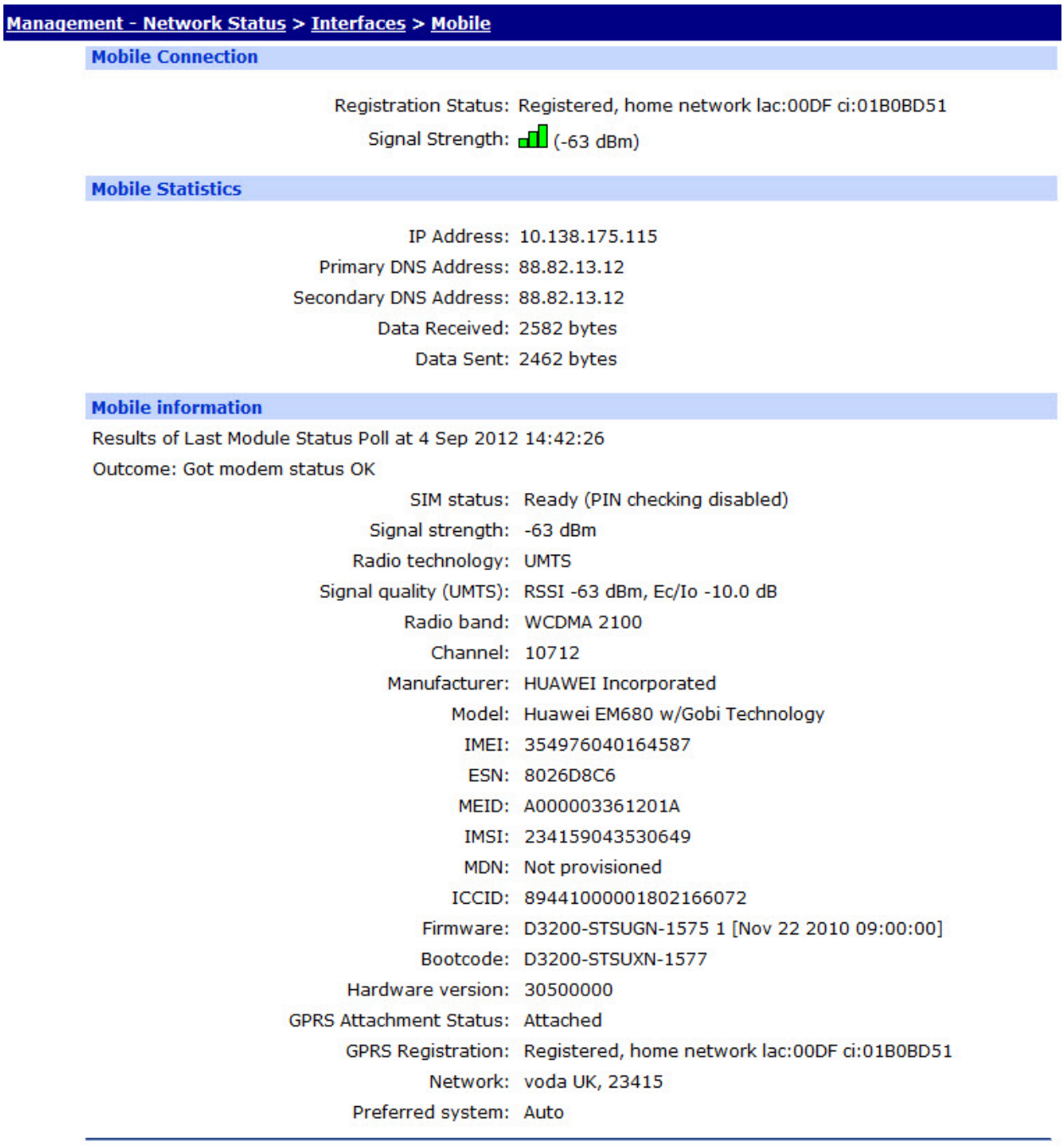
Related CLI Commands

Command	Options	Parameter	Equivalent Web Parameter
wificonn	n/a		Displays the Wi-Fi connection table.
wificonn	x	cscan	Performs wifi network scan
wifistat	n/a		Displays the Wi-Fi statistics.

Mobile

Management-Network Status> Interfaces> Mobile

The Mobile status page displays the current mobile connection, network and module information.


Management - Network Status > Interfaces > Mobile
Mobile Connection
Registration Status: Registered, home network lac:00DF ci:01B0BD51
Signal Strength: (-63 dBm)
Mobile Statistics
IP Address: 10.138.175.115
Primary DNS Address: 88.82.13.12
Secondary DNS Address: 88.82.13.12
Data Received: 2582 bytes
Data Sent: 2462 bytes
Mobile information
Results of Last Module Status Poll at 4 Sep 2012 14:42:26
Outcome: Got modem status OK
SIM status: Ready (PIN checking disabled)
Signal strength: -63 dBm
Radio technology: UMTS
Signal quality (UMTS): RSSI -63 dBm, Ec/Io -10.0 dB
Radio band: WCDMA 2100
Channel: 10712
Manufacturer: HUAWEI Incorporated
Model: Huawei EM680 w/Gobi Technology
IMEI: 354976040164587
ESN: 8026D8C6
MEID: A0000033612O1A
IMSI: 234159043530649
MDN: Not provisioned
ICCID: 89441000001802166072
Firmware: D3200-STSUGN-1575 1 [Nov 22 2010 09:00:00]
Bootcode: D3200-STSUXN-1577
Hardware version: 30500000
GPRS Attachment Status: Attached
GPRS Registration: Registered, home network lac:00DF ci:01B0BD51
Network: voda UK, 23415
Preferred system: Auto

Mobile Connection

Registration Status

The GSM registration status of the mobile module with respect to the GSM network. It may be one of the following

- Not Registered, not searching
- Not registered, searching
- Registered, home network
- Registered, roaming
- Registration denied
- Unknown
- ERROR

The registration status may sometimes be followed by additional information about the Location Area Code (LAC) and the Cell Identifier (CI).

Signal Strength
The signal strength in dBm being received by the mobile module. The range is -113dBm (min) to -51dBm (max). The signal strength bars should match the Signal Strength LEDs on the front of the router.

Mobile Statistics

IP Address
The IP address of the mobile interface.

Primary DNS Address / Secondary DNS Address
The primary and secondary DNS addresses used by the mobile interface.

Data Received
The number of data bytes that have been received on the mobile interface whilst it has been connected.

Data Sent
The number of data bytes that have been sent on the mobile interface whilst it has been connected.

Mobile Information

For GSM networks, the Mobile Information section can have the following items.

SIM Status
This indicates whether or not a valid SIM card has been installed in the router. It may be one of the following

- READY - SIM is OK
- SIM PIN - PIN number required
- SIM PUK - SIM blocked (unblocking code required)
- ERROR - SIM is not installed or is faulty

Radio Technology
The current network technology in use. It may be one of the following

- GSM
- GPRS
- EDGE
- UMTS
- HSDPA
- HSUPA
- CDMA

Manufacturer
The manufacturer of the mobile module.

Model
The model of the mobile module.

IMEI
The International Mobile Equipment Identification (IMEI) of the mobile module.

ESN
The Electronic Serial Number (ESN) of the mobile module.

MEID
The Mobile Equipment Identifier (MEID) of the mobile module.

IMSI
The International Mobile Subscriber Identity (IMSI) of the mobile module.

ICCID
This field specifies Integrated Circuit Card Identifier (ICCID) of the SIM card.

Firmware
This specifies firmware running on mobile module.

Bootcode
This field specifies bootcode firmware running on the mobile module.

Hardware Version
This specifies the hardware version of the mobile module.

GPRS Attachment Status
This is the current status of the mobile module with respect to the Mobile service. It may be one of the following

- Not attached - the unit has not connected to a mobile service.
- Attached - the unit has connector to a mobile service.
- ERROR - unknown response from the mobile module.

GPRS Registration
See Registration Status.

Network
The name of the GSM network to which the mobile module is currently connected to or ERROR if no network is available.

Preferred system
The preferred technology. It can be one of following

- Auto
- GSM only
- WCDMA only

For CDMA networks, the Mobile Information can have the following items.

Current system ID
The current system ID reported by the mobile module.

Current network ID
The current network ID reported by the mobile module.

Network
The current network reported by the mobile module.

Signal strength 1xRTT
The signal strength in dBm being received by the mobile module from 1xRTT networks.

Signal strength EVDO

The signal strength in dBm being received by the mobile module from EVDO networks.

Manufacturer
The manufacturer of the mobile module.

Model
The model of the mobile module.

MDN
The Mobile Directory Number (MDN) of the mobile module.

MIN
The Mobile Identification Number (MIN) of the mobile module.

ESN
The Electronic Serial Number (ESN) of the mobile module.

MEID
The Mobile Equipment Identifier (MEID) of the mobile module.

Firmware
The firmware running on mobile module.

Bootcode
The bootcode firmware running on the mobile module.

Hardware version
The hardware version of the mobile module.

Registration State
See Registration Status.

Roaming status
The current roaming status of the mobile module.

Radio interfaces in use
It can be one of the following

- CDMA 1x
- EVDO
- No service
- Unknown

PRL version
The version of the Preferred Roaming List (PRL) loaded on the mobile module.

Activation status
The activation state of the mobile module. It can be of the following

- 0 – Not activated
- 1 – Activated

Related CLI Commands

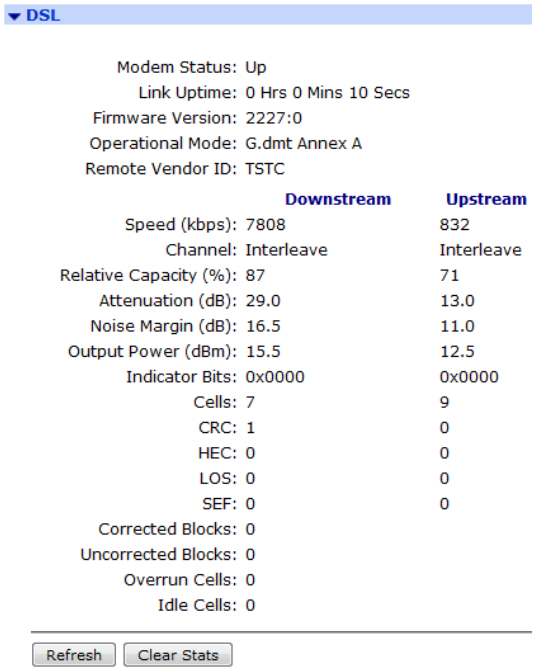
Command	Option	Equivalent Web Parameter
modemstat	?	Mobile Information
modemstat	s	Scan for Networks
pppstat	n	Mobile Statistics (where n is the PPP interface being used by the mobile interface)
at\mibs=ppp.n.stats	n	Displays the current interface statistics

Command	Option	Equivalent Web Parameter
at\mibclr=ppp.n.stats	n	Clears the current interface statistics

DSL

Management-Network Status> Interfaces > DSL

This page displays the current status and statistics of the DSL interface.



Modem Status
The current status of the DSL modem. On the DR64 platform, the values can be one of the following

- Idle
- Activating
- Ghs
- Training
- Up

Link Uptime
The amount of time the modem has been in the Up state.

Firmware Version
The version of the firmware running on DSL modem.

Operational Mode
The operational mode that the DSL modem is in when in the Up state. It is in the format of

<Mode> Annex <A | B | M>

where the <Mode> can be one the following

- ANSI

- ETSI
- G.dmt
- G.lite
- ADSL2
- ADSL2+

Remote Vendor ID
The remote vendor ID of the DSLAM that the DSL interface connected to.

Speed
The current speed the downstream and upstream DSL channels in Kbps.

Channel
The channel type being used. It can be either “Fast” or “Interleaved”.

Relative Capacity
The current relative capacity on the downstream and upstream DSL channels. The relative capacity is the percentage of your overall available bandwidth used to obtain your ATM service rate.

Attenuation
The current attenuation, in decibels, on the downstream and upstream DSL channels. Attenuation is the measure of how much the signal has degraded between the DSLAM and the DSL modem. The lower the attenuation, the better the performance will be.

Noise Margin
The current noise margin, in decibels, on the downstream and upstream DSL channels. The noise margin (aka Signal to Noise Ratio) is the relative strength of the DSL signal to noise. The larger the noise margin, the better the performance will do. In some instances, interleaving can help raise the noise margin.

Power Output
The current amount of power, in dBm, that the DSL modem (upstream) and DSLAM (downstream) are using. The lower the power output, the better the performance will be.

Indicator Bits
The indicator bit values being used on the downstream and upstream DSL channels.

Cells
The number of cells that have received (downstream) and transmitted (upstream).

CRC
The number of CRC errors that have occurred downstream and upstream.

HEC
The number of Header Error Controls (HEC) errors that have occurred downstream and upstream.

LOS
The number of Loss of Signal (LOS) errors that have occurred downstream and upstream.

SEF
The number of Severely Errored Frame (SEF) errors that have occurred downstream and upstream.

Corrected Blocks
The number of blocks that have been received and corrected by the forward error correction (FEC) code.

Uncorrected Blocks

The number of blocks that have been received and could not be corrected by the forward error correction (FEC) code.

Overrun Cells
The number of cells lost because of overrun errors.

Idle Cells
The number of idle cells received.

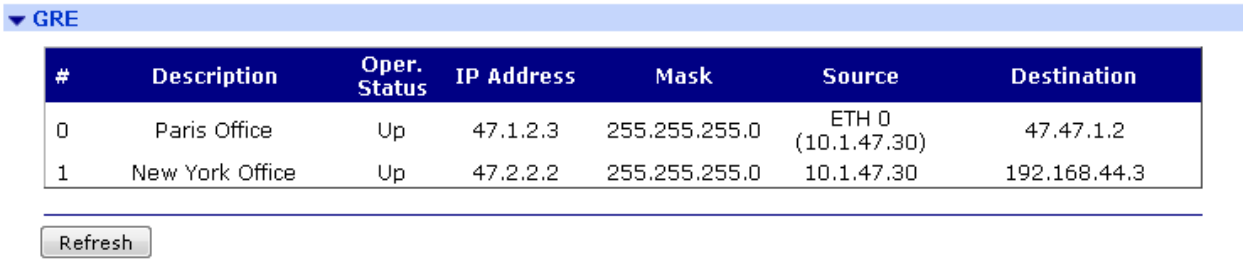
Related CLI Commands

Command	Instance	Equivalent Web Parameter
adslst	n/a	Displays the current DSL interface status.
at\mibs=adsl.0.stats	n/a	Displays the current DSL interface statistics.
at\mibclr=adsl.0.stats	n/a	Clears the current DSL interface statistics.
pppstat	n	DSL Statistics (where n is the PPP interface being used by the DSL PVC).

GRE

Management-Network Status> Interfaces > GRE

This page displays a summary table of the configured GRE interfaces.


GRE
Description Oper. Status IP Address Mask Source Destination
0 Paris Office Up 47.1.2.3 255.255.255.0 ETH 0 (10.1.47.30) 47.47.1.2
1 New York Office Up 47.2.2.2 255.255.255.0 10.1.47.30 192.168.44.3
Refresh

#
This indicates GRE interface number.

Description
The configured GRE interface description.

Oper. Status
The current operational status of the GRE interface. It can be one of the following values

Up	The GRE interface is up.
Lower Layer Down	The GRE interface has keepalives enabled but is not getting any response from the configured destination.

IP Address
The configured IP address for the GRE interface.

Mask
The configured IP subnet mask for the GRE interface.

Source
The configured source IP address or interface of the GRE interface.

Destination

The configured destination IP address or domain name of the GRE interface.

Further information on particular GRE interfaces can be obtained by selecting the appropriate GRE interface submenu underneath the GRE summary table.

As well as the above information, the following statistics are also displayed.

Bytes Received
The number of bytes that have been received on the GRE interface.

Bytes Sent
The number of bytes that have been sent on the GRE interface.

Packets Received
The number of packets that have been received on the GRE interface.

Packets Sent
The number of packets that have been sent on the GRE interface.

Keepalives Received
The number of GRE keepalive packets that have been received on the GRE interface.

Keepalives Sent
The number of GRE keepalive packets that have been sent on the GRE interface.

Rx Errors
The number of receive errors that have occurred on the GRE interface. These can include the received being an invalid GRE packet.

Tx Errors
The number of transmit errors that have occurred on the GRE interface. These can include an internal error due to no packet buffers being available.

Rx Unknown
The number of packets that have been received with an unknown IP protocol and have been dropped.

Tx Discards
The number of packets that have been discarded during transmission due to the GRE interface not being up or if a routing loop has been detected.

Related CLI Commands

Entity	Instance	Options	Equivalent Web Parameter
tunstat	n	n/a	Displays the GRE interface specific status and statistics.
tunstat	n	clear	Clears the statistics for the GRE interface.

ISDN

Management-Network Status> Interfaces > ISDN

This section contains the status information for the ISDN interface.

ISDN BRI

Management-Network Status> Interfaces> ISDN BRI

The status information is presented as a simple table having three or four columns as described below:

Channel
There are three supported channels; the D-channel, B1 and B2 channels that appear in this column. Each channel row has an associated status, protocol and (for data channels) action. The Action column will only appear when the associated channel becomes active.

Status
The status of each channel is shown in this column. The status is either ON or OFF.

Protocol
The protocol in use by the channel is shown in this column. This should be as set up in the configuration procedure. For D-channels, this will be LAPD. If the associated channel is not active, this entry will be blank.

Action
When the link becomes active, a button should appear in this column. The text on the button will be “Drop Link”. Clicking the button will deactivate the channel.

Related CLI Commands

If a PPP instance has been associated with a B-channel, the statistics for that PPP instance will be available using the normal `pppstat` **command.PSTN**

This section contains the network status information for the PSTN interface.

Link Name
If a description of the interface has been assigned during the configuration, it will appear here.

This PSTN interface is using PPP n
When configuring the PSTN module, a PPP instance is assigned – the instance number of the assigned PPP interface appears here.

IP Address
The IP address assigned to the interface is shown here.

Mask
This value is the subnet mask being used by the interface.

DNS Server
The IP address of the DNS server being used by the interface appears here.

Bytes Received
This value is the number of bytes received by the interface.

Bytes Sent
This value is the number of bytes sent by the interface.

LCP Packets Received
This value is the number of Link Control Protocol (LCP) packets received.

LCP Packets Sent
This value is the number of LCP packets sent by the interface.

PAP Packets Received
This value is the number of Password Authentication Protocol (PAP) packets sent by the interface.

PAP Packets Sent
This value is the number of PAP packets sent by the interface.

IPCP Packets Received
This value is the number of IP Control Protocol (IPCP) packets received by the interface.

IPCP Packets Sent
This value is the number of IPCP packets sent by the interface.

Receive Errors
This value indicates the number of frames received that contain an error (CRC etc).

Transmit Errors
This value indicates the number of frames that the interface attempted to transmit, but were found to contain an error.

Refresh
Clicking this button causes the status page to be refreshed with the updated statistics.

Clear PPP n Statistics
Clicking this button causes the statistics to be reset to zero.

Related CLI Commands

The CLI commands are the same as for other interfaces and are described in the PPP status section. The command to obtain the status is:

pppstat <n>

where <n> is the interface number for the PPP interface assigned to the PSTN module and is shown at the top of the web page**.**

Serial > Serial n

Management-Network Status> Interfaces> Serial> Serial n

This page displays the current status and statistics of the selected Serial interface.

DTR
The current status of the Data Terminal Ready (DTR) signal.

Bytes Received
The number of bytes that have been received on the serial interface.

Rx Overruns
The number of receive overruns that have occurred on the serial interface. A receive overrun occurs when there are not enough buffers to receive incoming data which results in the received data being dropped.

Tx Underruns
The number of transmit underruns that have occurred on the serial interface. A transmit underrun occurs when there is not enough data available when it is about to be transmitted.

Breaks Received
The number of times a break signal has been received.

Framing Errors Received
The number of framing errors that have been detected when receiving data on the serial interface.

Parity Errors Received
The number of parity errors that have been detected when receiving data on the serial interface.

Buffer Shortages

The number of times data that has been received on the serial interface has been dropped because of a lack of system buffers.

Message Shortages
The number of times data that has been received on the serial interface has been dropped because of a lack of system messages.

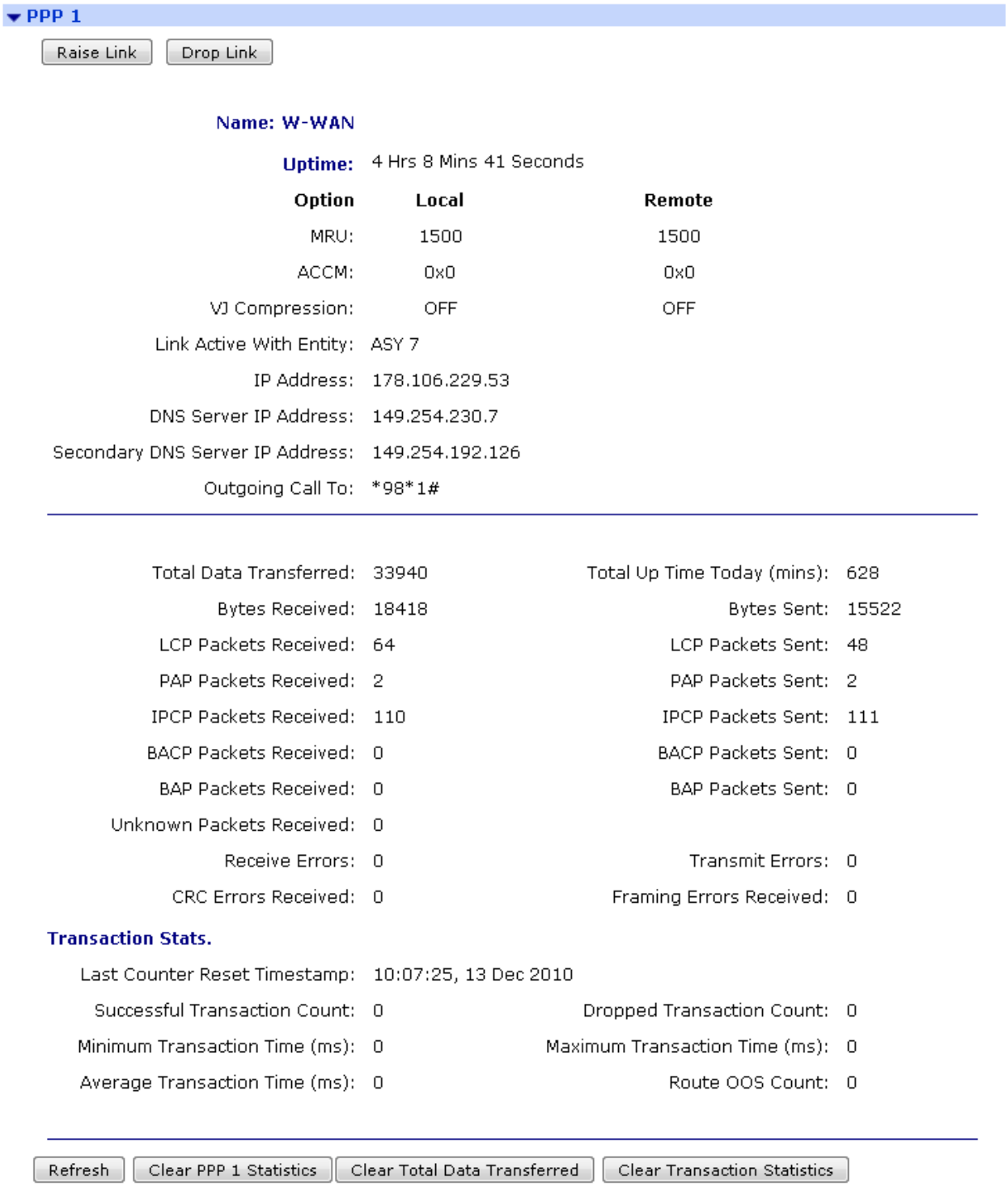
Related CLI Commands

Command	Instance	Parameter	Equivalent Web Parameter
at\mibs=asy.n	n/a	n/a	Displays the statistics for serial interface n.
at\mibclr=asy.n	n/a	n/a	Clears the statistics for serial interface n.

Advanced > PPP > PPP n

Management-Network Status> Interfaces> Advanced > PPP > PPP n

This page displays the current status and statistics of the selected PPP interface.



Name
The name assigned to the PPP interface.

Uptime
The amount of time the PPP interface has been up.

MRU
The maximum receive unit (MRU) that has been negotiated by each peer on the PPP connection.

ACCM
The Asynchronous Control Character Map (ACCM) that has been negotiated by each peer on the PPP connection.

VJ Compression
The Van Jacobson (VJ) compression that has been negotiated by each peer on the PPP connection.

Link with Active Entity
The entity that this PPP interface is using for connectivity.

IP Address
The IP address that has been assigned to this PPP interface. This could be either statically configured or assigned by the remote PPP peer.

DNS Server IP Address / Secondary DNS Server IP Address
The primary and secondary DNS server IP addresses that are being used by the PPP interface.

Outgoing Call To
If this is dial-out PPP interface, this is the number it used to make the call.

Total Data Transferred
The total amount of data bytes received and transmitted on the PPP interface including PPP headers and payload.

Total Up Time Today
The total amount of time in minutes that the PPP interface has been connected in the current 24 hour period.

Bytes Received
The number of bytes that have been received on the PPP interface.

Bytes Sent
The number of bytes that have been sent on the PPP interface.

LCP Packets Received
The number of Link Control Protocol (LCP) packets that have been received on the PPP interface.

LCP Packets Sent
The number of Link Control Protocol (LCP) packets that have been sent on the PPP interface.

PAP Packets Received
The number of Password Authentication Protocol (PAP) packets that have been received on the PPP interface.

PAP Packets Sent
The number of Password Authentication Protocol (PAP) packets that have been sent on the PPP interface.

IPCP Packets Received
The number of IP Control Protocol (IPCP) packets that have been received on the PPP interface.

IPCP Packets Sent
The number of IP Control Protocol (IPCP) packets that have been sent on the PPP interface.

BACP Packets Received
The number of Bandwidth Allocation Control Protocol (BACP) packets that have been received on the PPP interface.

BACP Packets Sent
The number of Bandwidth Allocation Control Protocol (BACP) packets that have been sent on the PPP interface.

BAP Packets Received
The number of Bandwidth Allocation Protocol (BAP) packets that have been received on the PPP interface.

BAP Packets Sent
The number of Bandwidth Allocation Protocol (BAP) packets that have been sent on the PPP interface.

Unknown Packets Received
The number of packets received with an unknown or unsupported PPP protocol.

Receive Errors
The number of receive errors that have occurred on the PPP interface.

Transmit Errors
The number of transmit errors that have occurred on the PPP interface.

CRC Errors Received
The number of packets that have been received on the PPP interface with invalid CRCs.

Framing Errors Received
The number of packets that have been received on the PPP interface with invalid framing.

Transaction Stats

Last Counter Reset Timestamp
The time when the PPP transaction statistics where last reset.

Successful Transaction Count
The number of successful PPP transactions.

Dropped Transaction Count
The number of transactions sent but no response has been received.

Minimum Transaction Time
The shortest response time in milliseconds for a PPP transaction.

Maximum Transaction Time
The longest response time in milliseconds for a PPP transaction.

Average Transaction Time
The average response time in milliseconds for the successful PPP transactions.

Route OOS Count

The number of Route “Out Of Service” messages sent by the firewall to the routing code. These messages put routes out of service for a period of time and are sent when enough failed PPP transactions have occurred.

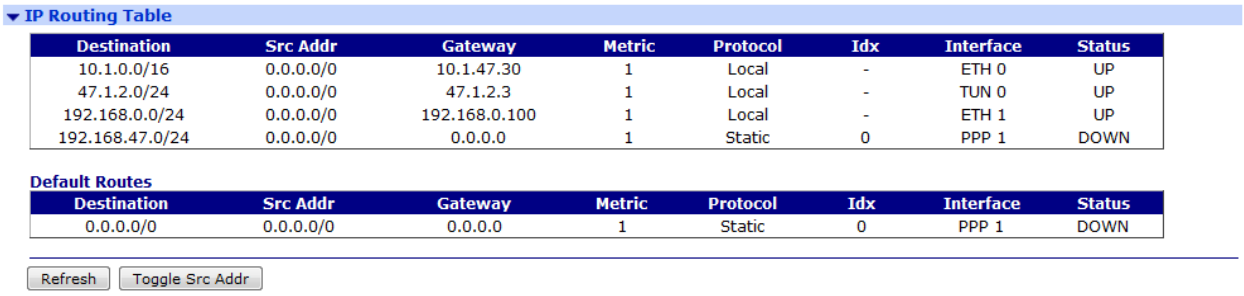
Related CLI Commands

Command	Instance	Parameter	Equivalent Web Parameter
ppp	n	status	Displays the current status of PPP interface n.
at\mibs=ppp.n.stats	n/a	n/a	Displays the statistics for PPP interface n.
at\mibclr=ppp.n.stats	n/a	n/a	Clears the statistics for PPP interface n.

IP Routing Table

Management-Network Status> IP Routing Table

This page displays the IPv4 routing table.


IP Routing Table
Destination Src Addr Gateway Metric Protocol Idx Interface Status
10.1.0.0/16 0.0.0.0/0 10.1.47.30 1 Local - ETH 0 UP
47.1.2.0/24 0.0.0.0/0 47.1.2.3 1 Local - TUN 0 UP
192.168.0.0/24 0.0.0.0/0 192.168.0.100 1 Local - ETH 1 UP
192.168.47.0/24 0.0.0.0/0 0.0.0.0 1 Static 0 PPP 1 DOWN
Default Routes
Destination Src Addr Gateway Metric Protocol Idx Interface Status
0.0.0.0/0 0.0.0.0/0 0.0.0.0 1 Static 0 PPP 1 DOWN
Refresh
Toggle Src Addr

Destination

The destination IP network of the route. The destination needs to match the destination IP address of an IP packet for the route to be used.

For default routes, the destination IP network is always 0.0.0.0/0. Default routes are used when no other route matches the destination IP address of an IP packet.

Src Addr

When source address routing is being used, the src addr needs to match the source IP address of an IP packet for the route to be used.

Gateway

The IP address of the next router to which the IP packet will be routed to in order to reach the destination network.

On PPP and TUN interfaces and ETH interfaces that have the gateway configured, this parameter can be blank.

Metric

The route metric defines the “cost” of the route. If CIDR routing is enabled and there are two routes to the same destination, the route with the lower metric is used.

Protocol

The protocol that created the route. It can be one of the following

Local	The route is for a network connected directly to the router.
Remote	The route is for a remote network accessed via a PPP connection.
Static	The route is a static route.
Static/RIP	The route is a static route that has been updated by RIP.
RIP	The route is a RIP route.
IBGP	The route is an interior BGP route.
EBGP	The route is an exterior BGP route.
OSPF	The route is an OSPF route.

Idx
This parameter is only used for static routes and it defines the index of the configured static route.

Interface
The interface over which the IP packet will be routed when the route is used.

Status
The current status of the route. It can be one of the following

UP	The route is up and can be used for routing.
DOWN	The interface that the route uses is currently down. The interface can be activated if the route is required.
OOS	The interface that the route uses is currently “Out of Service”.

Related CLI Commands

Command	Options	Equivalent Web Parameter
route	print	Displays the IPv4 routing table.
route	printsrc	Displays the IPv4 routing table with the src addr information.

IP Hash Table

Management-Network Status> Interfaces > IP Hash Table

The router uses a routing hash table to improve IPv4 routing performance by reducing route lookup times.

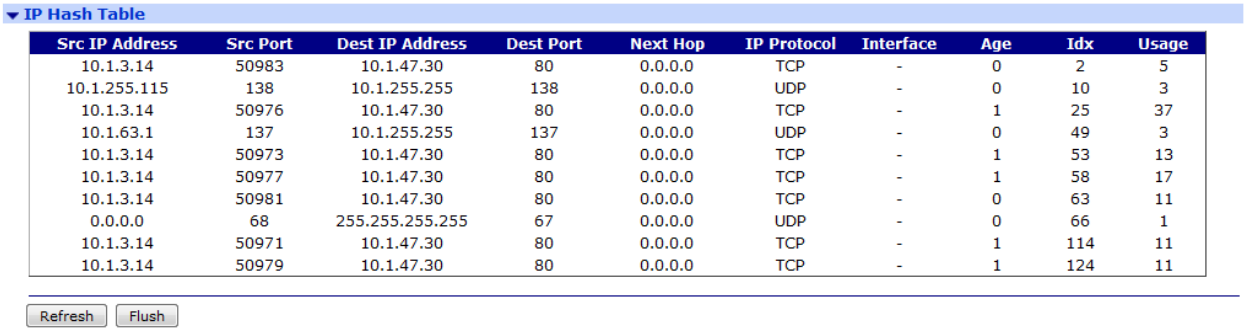
The IP hash table contains information on recently routed IP packets such as source and destination IP address, IP protocol, etc. It also contains information on the interface and gateway used when routing the IP packet.

When the router receives an IP packet to route, it will look in the IP hash table before looking in the IPv4 routing table.

Whenever the IPv4 routing table changes (e.g. a route is added, deleted or modified), all entries in the IP hash table are flushed out.

The IP hash table can be flushed manually using the “Flush” button.

Entries in the IP hash table are automatically deleted if it is not used for 10 seconds.



Src IP Address
The source IP address of the routed IP packet.

Src Port
The source TCP/UDP port of the routed IP packet. If the IP protocol is not TCP or UDP, then this field is “0”.

Destination IP Address
The destination IP address of the routed IP packet.

Dest Port
The destination TCP/UDP port of the routed IP packet. If the IP protocol is not TCP or UDP, then this field is “0”.

Next Hop
The next hop gateway to which the routed IP packet was sent to.

IP Protocol
The IP protocol field in the routed IP packet.

Interface
The interface that was used when the IP packet was routed.

Age
The age in seconds of the entry in the IP hash table.

Idx
The index in the IP hash table of the entry.

Usage
The number of times the entry has been used.

Related CLI Commands

Command	Options	Equivalent Web Parameter
route	hash	Displays the IP hash table.
route	flush	Flushes the IP hash table.

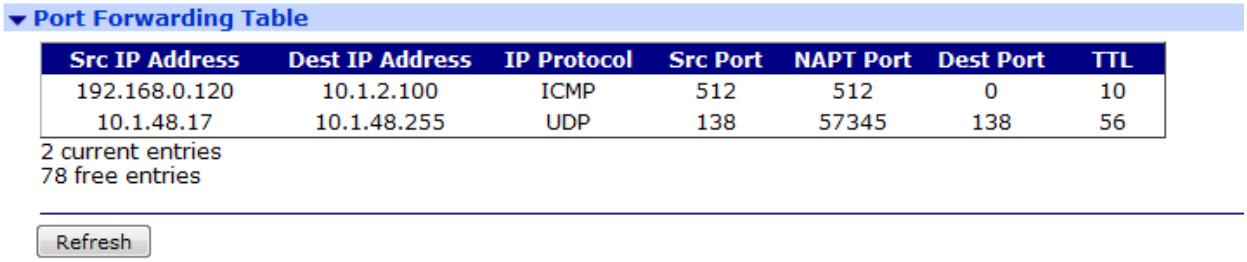
Port Forwarding Table

Management-Network Status> Port Forwarding Table

This page displays the Port Forwarding / NAT table.

The Port Forwarding table is used by the router to keep track of IP packets that have been modified via NAT or NAPT in to order to be routed over a particular network.

When the router receives a response to a previously modified IP packet, it will look up the matching entry in the Port Forwarding table in order to correctly modify the response IP packet.



Src IP Address
The source IP address of the modified IP packet.

Dest IP Address
The destination IP address of the modified IP packet.

IP Protocol
The IP protocol field of the modified IP packet.

Src Port
The source TCP/UDP port of the modified IP packet. For ICMP packets, this defines the ICMP Echo identifier value.

NAPT Port
The new destination TCP/UDP of the modified IP packet. For ICMP packets, this defines the ICMP Echo identifier value.

Dest Port
The original destination TCP/UDP port of the modified IP packet.

TTL
The time to live in seconds for the Port Forwarding entry. If the entry is not used for the specified amount of time, the entry is deleted from the Port Forwarding table.

Related CLI Commands

Command	Options	Equivalent Web Parameter
nat	list	Displays the Port Forwarding / NAT table.

Firewall

Management-Network Status> Firewall

This page displays the current Firewall statistics and the Firewall Stateful Inspection table.

Passed Packets
The number of packets the firewall has passed.

Blocked Packets
The number of packets the firewall has blocked.

Logged Packets
The number of packets the firewall has logged.

Stateful Packets
The number of packets that have matched a stateful rule.

Undersized Packets
The number of packets received by the firewall that are too small.

Oversized Packets
The number of packets received by the firewall that are too large.

Return TCP RST
The number of times the firewall has returned a TCP Reset packet.

Return ICMP
The number of times the firewall has returned an ICMP packet.

Stateful rule shortages
The number of times there has been a shortage of entries stateful inspection table.

HASH table errors
The number of times there has been a hashing error when looking into the stateful inspection table.

In use stateful rules reused
The number of times an in-use stateful inspection table has been reused.

Firewall Stateful Inspection Table

The Firewall Stateful Inspection table is a sophisticated scripted “Stateful Firewall” and “Route Inspection” engine. Stateful inspection is a powerful tool that allows the unit to keep track of a TCP/UDP or ICMP session and match packets based on the state of the connection on which they are being carried.

The table contains a list of dynamic firewall rules that have been created when packets have matched a configured firewall with the ***inspect-state*** keyword specified.

For more information on the ***inspect-state*** keyword, see “Stateful Inspection” in the Firewall section.

TTL	Hits	Direction	Src IP Addr	Src Port	Dst IP Addr	Dst Port	Trans. Src IP Addr	Trans. Src Port	Trans. Dst IP Addr	Trans. Dst Port	Protocol	Interface
7	2	OUT	213.152.58.85	1093	212.104.130.9	53	0.0.0.0	0	0.0.0.0	0	UDP	PPP 1

Refresh

TTL
The number of seconds for the table entry to live. When this reaches zero, the entry is removed from the table.

Hits
The number of times an IP packet has been matched against the firewall rule.

Direction
The direction of the IP packets that match the firewall rule.

Src IP Addr
The source IP address of the IP packets that match the firewall rule.

Src Port
The source TCP/UDP port of the IP packets that match the firewall rule.

Dest IP Addr
The destination IP address of the IP packets that match the firewall rule.

Dest Port
The destination TCP/UDP port of the IP packets that match the firewall rule.

Trans. Src IP Addr
If the firewall is configured to modify (e.g. NAT or NAPT) the source IP address of the IP packets that match the firewall, this defines the new source IP address of the IP packets.

Trans. Src Port
If the firewall is configured to modify (e.g. NAPT) the source TCP/UDP port of the IP packets that match the firewall, this defines the new source TCP/UDP port of the IP packets.

Trans. Dest IP Addr
If the firewall is configured to modify (e.g. NAT or NAPT) the destination IP address of the IP packets that match the firewall, this defines the new destination IP address of the IP packets.

Trans. Dest Port
If the firewall is configured to modify (e.g. NAPT) the destination TCP/UDP port of the IP packets that match the firewall, this defines the new destination TCP/UDP port of the IP packets.

Protocol
The IP protocol of the IP packets that match the entry.

Interface
The interface over which the IP packets that match the entry are sent or received.

Related CLI Commands

Command	Options	Equivalent Web Parameter
fwall	show	Displays the Firewall Stateful Inspection table.

Firewall Trace

Management-Network Status> Firewall Trace

The firewall trace output is appended to when the ***log*** keyword is used in the firewall.

Most commonly, the ***log*** keyword is used in the last rule in form ***block log break end*** to log a summary of all packets that did not match one of the preceding allow rules.

The ***log*** keyword is much more versatile in its usage and what can be logged. For more information see “log:” in the Firewall Scripts section.

An example output is show below, this is from the commonly used firewall rule

block log break end

----- 5-10-2009 23:12:08 ------

FW LOG Dir: IN Line: 37 Hits: 4730 IFACE: ETH 3

Source IP: 222.45.112.59 Dest IP: 217.34.133.21 ID: 256 TTL: 106 PROTO: TCP (6)

Src Port: 12200 Dst Port: 8118

block log break end

----- 5-10-2009 23:13:15 ------

FW LOG Dir: IN Line: 37 Hits: 4731 IFACE: ETH 3

Source IP: 218.61.22.42 Dest IP: 217.34.133.21 ID: 35372 TTL: 136 PROTO: TCP (6)

Src Port: FTP CTL (21) Dst Port: 16794

block log break end

---

2 example logged packets are shown. The output of the 1st logged packet can be explained as follows:

----- 5-10-2009 23:12:08 ------
This is the time stamp of the blocked packet.

FW LOG Dir: IN Line: 37 Hits: 4730 IFACE: ETH 3
'Dir:' is the direction of the packet that was logged, either IN or OUT of the router.
'Line:' is the line number within the firewall rules that caused this packet to be logged.
'Hits:' is the number of packets that have matched this rule.
'IFACE:' is the interface which the packet was logged on.

Source IP: 222.45.112.59 Dest IP: 217.34.133.21 ID: 256 TTL: 106 PROTO: TCP (6)
'Source IP:' is the source IP address of the packet that was logged.
'Dest IP:' is the destination IP address of the packet that was logged.
'ID:' is the ID of the packet, this is taken from the packet header.
'TTL:' is the Time To Live value.
'PROTO:' is the layer 3 protocol of the logged packet.

Src Port: 12200 Dst Port: 8118
'Src Port' is the source TCP or UDP port number of the packet that was logged.
'Dst Port' is the destination TCP or UDP port number of the packet that was logged.

'block log break end' This is the actual rule that caused the packet to be logged.

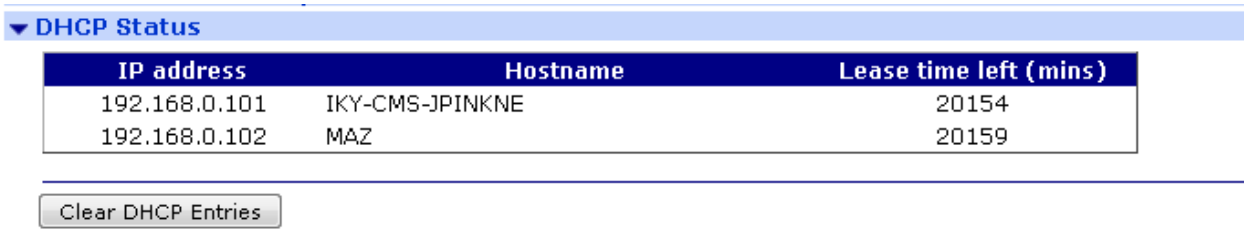
Related CLI Commands

Command	Options	Equivalent Web Parameter
type fwlog.txt	n/a	Displays the current Firewall trace.

DHCP Status

Management-Network Status> DHCP Status

This page displays the current DHCP status table.



IP Address
The IP address assigned to the hostname.

Hostname
The hostname to which the IP address has been assigned.

Lease time left (mins)
The length of time in minutes the IP address lease is valid for. After this time, the DHCP client will need to renew its IP address.

Mac Adress
This describes the MAC address

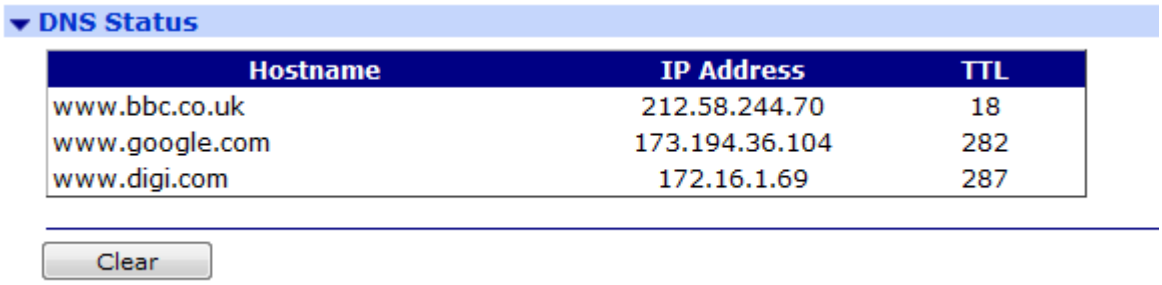
Related CLI Commands

Entity	Instance	Parameter	Equivalent Web Parameter
dhcp	0	status	Displays the current status of the DHCP table.
dhcp	0	clear	Deletes all the entries in the DHCP table.

DNS Status

Management-Network Status> DNS Status

This page displays DNS status table.



Hostname
The hostname that has been resolved.

IP Address
The IP address of the hostname.

TTL

The time to live in seconds for the DNS entry. When the TTL reaches zero, the entry is deleted.

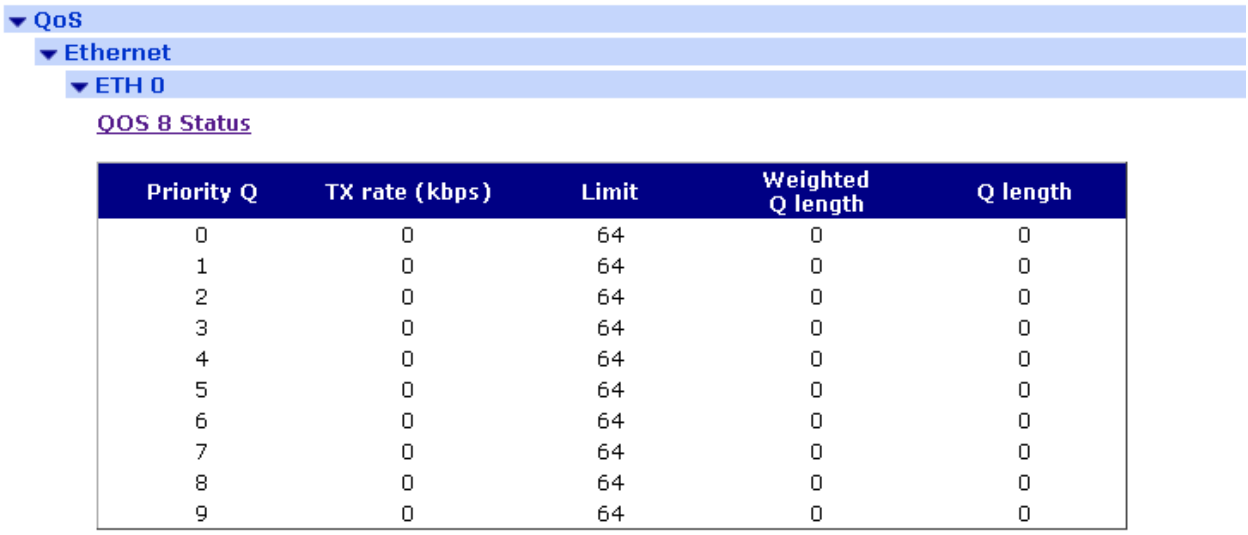
Related CLI Commands

Entity	Instance	Parameter	Equivalent Web Parameter
dns	0	status	Displays the current status of the DNS table.
dns	0	clear	Deletes all the entries in the DNS table.

QoS

Management-Network Status> QoS

This page displays the current QoS status table for a particular interface.



Priority Q	TX rate (kbps)	Limit	Weighted Q length	Q length
0	0	64	0	0
1	0	64	0	0
2	0	64	0	0
3	0	64	0	0
4	0	64	0	0
5	0	64	0	0
6	0	64	0	0
7	0	64	0	0
8	0	64	0	0
9	0	64	0	0

Priority Q
The priority queue in the table.

TX rate (kbps)
The current transmit rate in kbps of the queue.

Limit
The current transmit rate limit in kbps of the queue.

Weighted Q length
The weighted queue length using the Weighted Random Early Discard (WRED) algorithm.

Q length
The number of packets on the queue.

Connections Management

The ***Management- Connections*** webpage has the following menu options:

- IP Connections
- PPP Connections
- Virtual Private Networking (VPN)

IP Connections

Management- Connections > IP Connections

This page displays the current status of the TCP sockets on the router.

The router has two types of sockets

TCP Sockets	Reserved for WEB and FTP connections.
General Purpose Sockets	Can be used by any application for TCP connections.

TCP Sockets

TCP Sockets

ID	SID	State	Local IP Addr	Local Port	Remote IP Addr	Remote Port
0	2	LISTEN	0.0.0.0	21	0.0.0.0	0
1	3	LISTEN	0.0.0.0	80	0.0.0.0	0
2	286	ESTAB	10.1.47.30	80	10.49.16.16	54209
3	-1	CLOSED Closed (FW2)	10.1.47.30	80	10.49.16.16	54207
4	-1	CLOSED Closed (FW2)	10.1.47.30	80	10.49.16.16	54191
5	-1	CLOSED Closed (FW2)	10.1.47.30	80	10.49.16.16	54194
6	-1	CLOSED Closed (FW2)	10.1.47.30	80	10.49.16.16	54196
7	-1	CLOSED Closed (FW2)	10.1.47.30	80	10.49.16.16	54197
8	-1	CLOSED Closed (FW2)	10.1.47.30	80	10.49.16.16	54198
9	-1	CLOSED Closed (FW2)	10.1.47.30	80	10.49.16.16	53754
10	-1	CLOSED Closed (FW2)	10.1.47.30	80	10.49.16.16	53755
11	0	LISTEN	0.0.0.0	0	0.0.0.0	0
12	0	LISTEN	0.0.0.0	0	0.0.0.0	0
13	0	LISTEN	0.0.0.0	0	0.0.0.0	0
14	0	LISTEN	0.0.0.0	0	0.0.0.0	0

SYNs waiting : 0
Free SYN entries : 40, min 35

ID
The TCP socket identifier.

SID
An internal socket identifier.

State
The current state of the socket.

Local IP Addr
The IP address on the router that is being used for the TCP connection.

Local Port
The TCP port on the router that is being used for the TCP connection or is being listened on.

Remote IP Address
The IP address of the remote device that has the TCP connection to the router.

Remote Port
The TCP port being used by the connected remote device.

SYNs Waiting
The number of TCP SYN packets that are currently being processed by the router.s

Free SYN entries
The number of entries available to process an incoming TCP SYN packet.

Related CLI Commands

Command	Options	Description
socks		Displays the current status of the TCP sockets.

General Purpose Sockets

General Purpose Sockets

ID	Owner	Protocol	Mode	State	Local Port	Remote IP Addr	Remote Port	Inactivity Timeout (secs)
0	ASY 0	TCP	Normal	Listening	4000			300
1	ASY 1	TCP	Normal	Listening	4001			300
2	ASY 2	TCP	Normal	Listening	4002			300
3	ASY 3	TCP	Normal	Listening	4003			300
4	ASY 4	TCP	Normal	Listening	4004			300
5	ASY 5	TCP	Normal	Listening	4005			300
6	ASY 6	TCP	Normal	Listening	4006			300
7	ASY 7	TCP	Normal	Listening	4007			300
8	ASY 8	TCP	Normal	Listening	4008			300
9	ASY 9	TCP	Normal	Listening	4009			300
10	ASY 10	TCP	Normal	Listening	4010			300
11	X25 75	TCP	XOT	Listening	1998			300
12	X25 76	TCP	XOT	Listening	1998			300
13	X25 77	TCP	XOT	Listening	1998			300
14	X25 78	TCP	XOT	Listening	1998			300
15	X25 79	TCP	XOT	Listening	1998			300
16	X25 80	TCP	XOT	Listening	1998			300
17	X25 81	TCP	XOT	Listening	1998			300
18	X25 82	TCP	XOT	Listening	1998			300
19	X25 83	TCP	XOT	Listening	1998			300
20	X25 84	TCP	XOT	Listening	1998			300
21	X25 85	TCP	XOT	Listening	1998			300
22	X25 86	TCP	XOT	Listening	1998			300
23	X25 87	TCP	XOT	Listening	1998			300
24	X25 88	TCP	XOT	Listening	1998			300
25	X25 89	TCP	XOT	Listening	1998			300
26	X25 90	TCP	XOT	Listening	1998			300
27	SSH 1	TCP	Normal	Listening	22			300
28	SSH 3	TCP	Normal	Listening	22			300
29	SSH 5	TCP	Normal	Listening	22			300
30	SSH 7	TCP	Normal	Listening	22			300
31	SSH 9	TCP	Normal	Listening	22			300
35	REALPORT 3	TCP	Normal	ESTAB	771	10.49.16.16	60564	300
43	CMD	TCP	Normal	Listening	23			300

Total Number of Sockets : 44
Number of Free Sockets : 10

ID

The ID of the general purpose socket.

Owner
The software task that created the socket.

Protocol
The protocol being used by the socket.

Mode
The mode of operation of the socket.

State
The current state of the socket.

Local Port
The port of the router that is being used by the socket.

Remote IP Addr
The IP address of the remote device that has a TCP connection with the socket.

Remote Port
The TCP port being used by the remote device.

Inactivity Timeout
The socket's inactivity timeout (in seconds). If the timer reaches zero seconds, the TCP connection is closed.

Total Number of Sockets
The total number of general purpose sockets available on the router.

Number of Free Sockets
The number of free general purpose sockets available on the router.

Related CLI Commands

Command	Options	Description
gpstat		Displays the current status of the general purpose sockets.
gpstat	close <ID>	Closes the GP Socket connection with the ID number specified.

Virtual Private Networking (VPN) Management

Management-Connections> VPN

The ***Management-Connections> VPN*** menu has the following sub-menu options:

- IPsec
- OVPN

IPsec

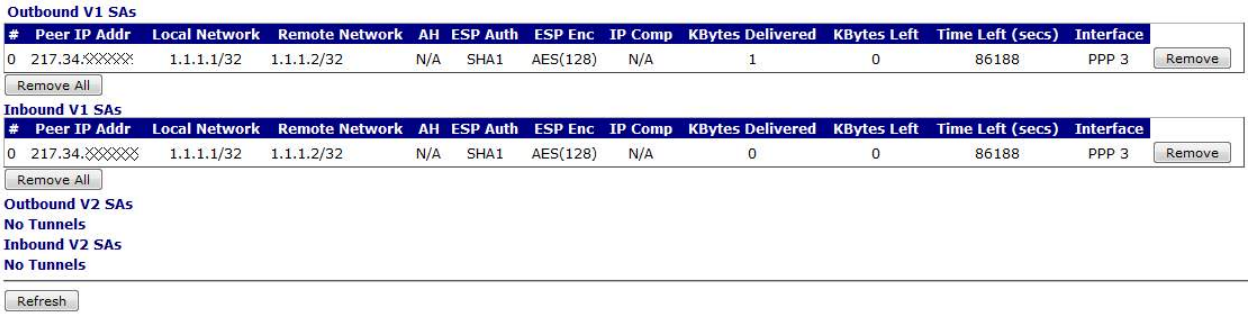
Management- Connections> VPN> IPsec

The ***Management- Connections> VPN> IPsec*** sub-menu has the following sub-menu options:

- IPsec Tunnels
- IPsec peers
- IKE SAs

IPsec Tunnels

This page displays the current status of the IPsec tunnels.


Outbound V1 SAs
Peer IP Addr Local Network Remote Network AH ESP Auth ESP Enc IP Comp KBytes Delivered KBytes Left Time Left (secs) Interface
0 217.34.XXXXX 1.1.1.1/32 1.1.1.2/32 N/A SHA1 AES(128) N/A 1 0 86188 PPP 3 Remove
Remove All
Inbound V1 SAs
Peer IP Addr Local Network Remote Network AH ESP Auth ESP Enc IP Comp KBytes Delivered KBytes Left Time Left (secs) Interface
0 217.34.XXXXX 1.1.1.1/32 1.1.1.2/32 N/A SHA1 AES(128) N/A 0 0 86188 PPP 3 Remove
Remove All
Outbound V2 SAs
No Tunnels
Inbound V2 SAs
No Tunnels
Refresh

#
IPsec tunnel number.

SPI
The Security Parameters Index (SPI) is a pointer that references the session key and algorithm used to protect the data in the IPsec tunnel.

Peer IP
The IP address of the remote device that is the other end of the IPsec tunnel.

Local Network
The local IP network of the IPsec tunnel that is connected to the router.

Remote Network
The remote IP network of the IPsec tunnel that is connected to the remote device.

First Rem. IP / Last Rem. IP
For IPsec tunnels that have been negotiated using IKEv2, this is the range IP addresses available on the remote IP network.

First Loc. IP / Last Loc. IP
For IPsec tunnels that have been negotiated using IKEv2, this is the range IP addresses available on the local IP network.

AH
The AH algorithm in use, if any.

ESP Auth
The ESP authentication algorithm in use, if any.

ESP Enc
The ESP encryption algorithm in use, if any.

IPComp
The data compression algorithm in use, if any.

KBytes Delivered
The total amount of data that has been transferred (in both directions) over this IPsec tunnel.

KBytes Left
The amount of data left to be transferred over the IPsec tunnel before the data duration limit is reached. The data duration is negotiated between the router and the remote device.

Time Left
The time left (in seconds) before the time duration limit is reached. The time duration is negotiated between the router and the remote device.

Interface
The interface over which the IPsec tunnel is on.

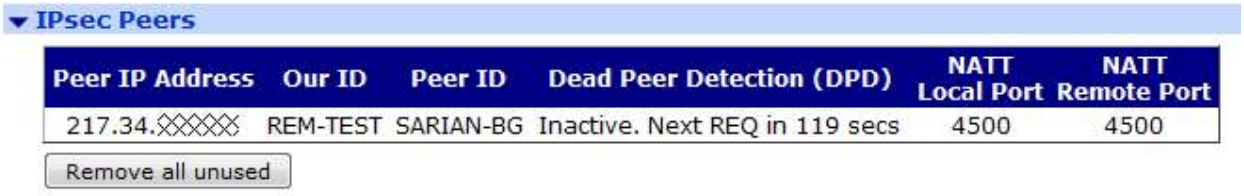
Related CLI Commands

Command	Options	Description
sastat	[dyn]	Displays the current status of all of the IPsecs tunnels. The optional "dyn" parameter can be used to display the status of the dynamic IPsec tunnels.
sastat	[dyn] <first> <last>	Displays the current status of the IPsec tunnels in the range from <first> to <last>. e.g. sastat 0 49 or sastat dyn 0 49
sastat	[dyn] peer <peer>	Displays the current status of the IPsec tunnels that match the given peer. The <peer> value can contain the '*' wildcard character. e.g. sastat peer uk-north-* or sastat dyn peer uk-north-*

IPsec peers

This page displays the current status of the IPsec peers.

This is the list of remote devices that have successfully negotiated an IPsec tunnel with the router.



Peer IP Address

The IP address of the remote device.

Our ID
The ID of the router.

Peer ID
The ID of the remote device.

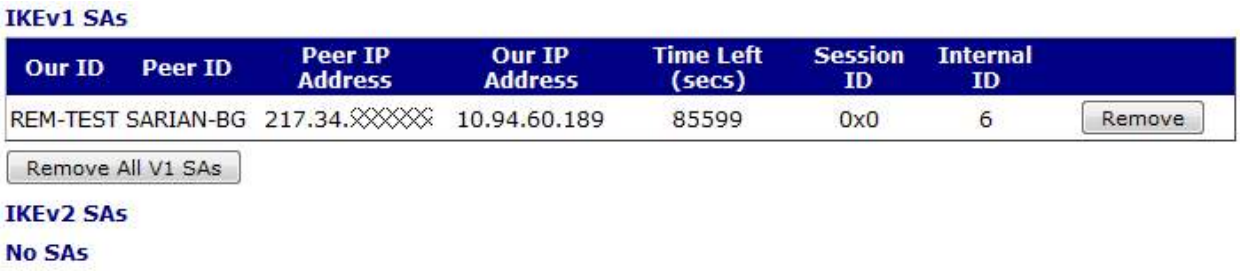
Dead Peer Detection (DPD)
The DPD status and the time until the next DPD request.

NATT Local Port
The local NAT-Traversal port.

NATT Remote Port
The remote NAT-Traversal port.

IKE SAs

This page displays the current status of the IKE Security Associations (SA).



Our ID
The ID of the router.

Peer ID
The ID of the remote device with which the IKE SA has been negotiated.

Peer IP Address
The IP address of the remote device.

Our IP Address
The IP address the router used to negotiate the IKE SA.

Time Left
The time remaining (in seconds) for the IKE SA to remain in force.

Session ID
The ID of the IKE SA.

Internal ID
An internal identifier for the IKE SA.

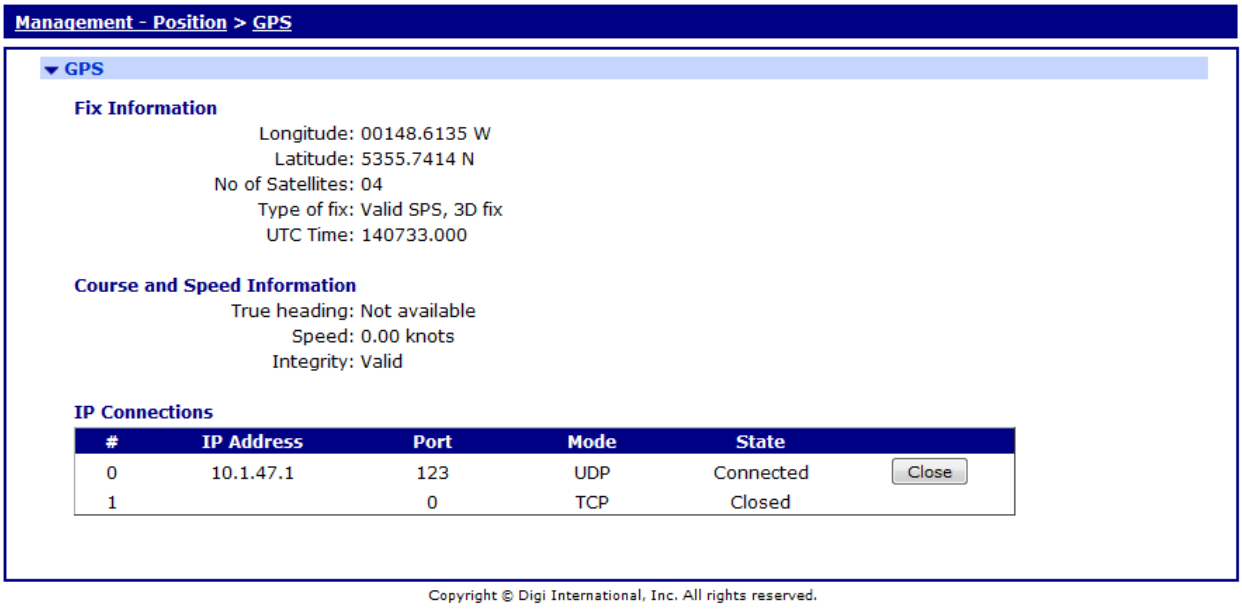
Position Management

The ***Management- Position*** webpage has ***GPS*** menu.

GPS

Management- Position > GPS

This page displays a summary of the most recent information received from the GPS module (if fitted) and the status of the IP connections.



Longitude
The current longitude contained in the last GGA, GLL or RMC message from the GPS module.

Latitude
The current latitude contained in the last GGA, GLL or RMC message from the GPS module.

No of Satellites
The current number of satellites being used as indicated in the last GGA message from the GPS module.

Type of fix
The current fix status as indicated in the last GGA, GLL or RMC message, followed by the type of fix (e.g. 2D, 3D or no fix) as indicated in the last GSA message.

UTC
The current UTC time as indicated in the last ZDA, GGA, GLL or RMC message from the GPS module.

True Heading
The current true heading as indicated in the last RMC message from the GPS module. If the router is not moving, this value is not available.

Speed
The current speed as indicated in the last RMC message from the GPS module.

Integrity

The current data integrity as indicated in the last RMC message from the GPS module. It can be either “Valid” or “Not Valid”.

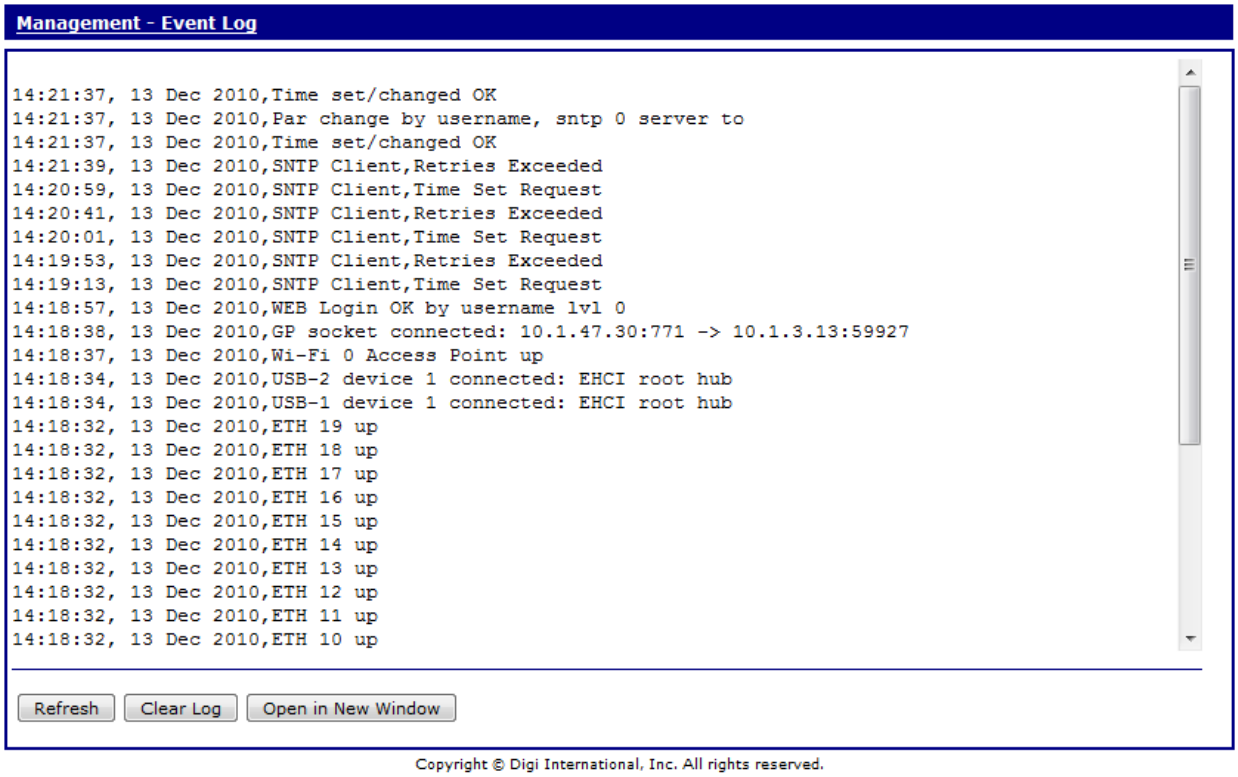
IP Connections
The current IP address, port number, connection type and status of the IP connections.

Related CLI Commands

Command	Options	Description
at\mibs=gps.0.stats		Displays the current status of the GPS receiver.

Event Log Management

The ***Management – Event Log*** page displays the current contents of the event log on the router.


Management - Event Log
14:21:37, 13 Dec 2010,Time set/changed OK
14:21:37, 13 Dec 2010,Par change by username, sntp 0 server to
14:21:37, 13 Dec 2010,Time set/changed OK
14:21:39, 13 Dec 2010,SNTP Client,Retries Exceeded
14:20:59, 13 Dec 2010,SNTP Client,Time Set Request
14:20:41, 13 Dec 2010,SNTP Client,Retries Exceeded
14:20:01, 13 Dec 2010,SNTP Client,Time Set Request
14:19:53, 13 Dec 2010,SNTP Client,Retries Exceeded
14:19:13, 13 Dec 2010,SNTP Client,Time Set Request
14:18:57, 13 Dec 2010,WEB Login OK by username lvl 0
14:18:38, 13 Dec 2010,GP socket connected: 10.1.47.30:771 -> 10.1.3.13:59927
14:18:37, 13 Dec 2010,Wi-Fi 0 Access Point up
14:18:34, 13 Dec 2010,USB-2 device 1 connected: EHCI root hub
14:18:34, 13 Dec 2010,USB-1 device 1 connected: EHCI root hub
14:18:32, 13 Dec 2010,ETH 19 up
14:18:32, 13 Dec 2010,ETH 18 up
14:18:32, 13 Dec 2010,ETH 17 up
14:18:32, 13 Dec 2010,ETH 16 up
14:18:32, 13 Dec 2010,ETH 15 up
14:18:32, 13 Dec 2010,ETH 14 up
14:18:32, 13 Dec 2010,ETH 13 up
14:18:32, 13 Dec 2010,ETH 12 up
14:18:32, 13 Dec 2010,ETH 11 up
14:18:32, 13 Dec 2010,ETH 10 up
Refresh
Clear Log
Open in New Window
Copyright © Digi International, Inc. All rights reserved.

The event log is stored in a pseudo-file called “eventlog.txt”. It acts as a circular buffer so that when there is no space available for new entries, the oldest entries are overwritten.

Each entry in the log normally consists of a single line containing the date, time and a brief description of the event. In some case it may also identify:

the type/number of the protocol instance the generated the message (e.g. PPP 0)

a reason code

Additional information such as an X.25 address or ISDN telephone number.

The specific events that generate a log entry are pre-defined and cannot be altered although the text and priority of each event can be modified. This can be done via the **Configuration - Alarms > Event Logcodes** page.

Related CLI Commands

Command	Options	Description
type eventlog.txt		Displays the contents of the event log.
clear_ev		Clears the contents of the event log.

Analyser Management

Management-Analyser

The router can be configured to capture a trace of the data being transmitted and received on the various interfaces. It is able to capture the layer 1, 2 and 3 protocol data and present it in an easily read format. The ***Management-Analyser*** page has the following menu options:

- Settings
- Trace
- PCAP (e.g. Wireshark) traces

Settings

Management-Analyser > Settings

Enable Analyser
This checkbox is used to enable or disable the analyser.

Maximum packet capture size
The number of bytes that are captured and stored for each packet. If the packet is bigger than the configured size, the packet is truncated. Bear in mind that the larger this value, the quicker the pseudo file “ana.txt” will become full so that the effective length of the analyser trace is reduced.

Log Size
The maximum size of the pseudo file “ana.txt” that is used to store the captured data packets. Once the maximum size is reached, the oldest captured data packets are overwritten when new packets are captured.
The maximum value is 180Kb, but the data is compressed so more than 180Kb of trace data will be captured.

Protocol layers
The checkboxes shown under this heading are used to specify which protocol layers are captured and included in the analyser trace. You can choose to capture Layer 1 (physical / PPP), Layer 2 (Laye protocol, the Network Layer (Layer 3) protocol or any combination, by checking or clearing the appropriate checkboxes. In addition, you may select XOT (X.25 over TCP/IP) tracing if this feature is included on the router.

Enable IKE debug
This checkbox is used to enable or disable the inclusion of IKE packets in the analyser trace when using IPsec.

Enable QMI trace
This checkbox is used to enable or disable the inclusion of data from the Qualcomm Management Interface in the analyser trace.

Enable SNAIP trace
This checkbox is used to enable or disable the inclusion of SNAIP packet in the analyser trace.

ISDN Sources
The checkboxes shown under this heading are used to select the ISDN channels (D, B1 and B2) over which packets will be captured and included in the analyser trace.

LAPB Links
The checkboxes shown under this heading are used to select the LAPB links over which packets will be captured and included in the analyser trace.

Serial Interfaces
The checkboxes shown under this heading are used to select the serial interfaces over which packets will be captured and included in the analyser trace. The list of available interfaces will include the physical serial interfaces, internal virtual serial interfaces (if present) and interfaces used by built-in WWAN and/or PSTN modems.

Ethernet Interfaces
The checkboxes shown under this heading are used to select the Ethernet interfaces over which packets will be captured and included in the analyser trace.

Raw SYNC Sources
The checkboxes shown under this heading are used to select the synchronous sources over which packets will be captured and included in the analyser trace.

DSL PVC Sources
The checkboxes shown under this heading are used to select the ADSL ATM PVCs over which packets will be captured and included in the analyser trace.

PPP Interfaces
The checkboxes shown under this heading are used to select the PPP interfaces over which packets will be captured and included in the analyser trace.

IP Sources
The checkboxes shown under this heading are used to select the IP sources over which packets will be captured and included in the analyser trace. These sources include IP packets transmitted and received over Ethernet, PPP and OpenVPN (OVPN) interfaces. It is also possible to select GRE Tunnels via the advanced sections of the individual GRE Tunnel configuration pages.

IP Options

Trace discarded packets
This checkbox is used to enable or disable the capture of packets that are discarded by an interface along with a reason for why the packet was discarded.

Trace loopback packets
This checkbox is used to enable or disable the capture of IP loopback packets.

IP Packet Filters / Discarded IP Packet Filters

TCP/UDP Ports
This parameter is used to filter out TCP or UDP packets with particular source or destination port numbers. The format of this parameter is a comma-separated list of port numbers. For example, you may wish to exclude the capture of Telnet and HTTP traffic that would otherwise swamp the data of interest. This can be done by entering “23,80” for this parameter.
Conversely, you may wish to only capture traffic on a specific source or destination port. To do this, use a tilde (~) symbol before the list of ports. For example, to only capture Telnet and SSH packets, enter “~22,23” for this parameter.

IP Protocols
This parameter is used to filter out IP packets with particular IP protocol numbers. The format of this parameter is a comma-separated list of protocol numbers. For example, you may wish to exclude the capture of TCP traffic that would otherwise swamp the data of interest. This can be done by entering “6” for this parameter.
Conversely, you may wish to only capture traffic with a specific IP protocol number. To do this, use a tilde (~) symbol before the list of protocol numbers. For example, to only capture UDP traffic, enter “~17” for this parameter.

IP Addresses

This parameter is used to filter out IP packets with particular source or destination IP addresses. The format of this parameter is a comma-separated list of IP addresses. For example, you may wish to exclude the capture of traffic from IP hosts 10.1.2.3 and 10.2.2.2. This can be done by entering "10.1.2.3,10.2.2.2" for this parameter. Conversely, you may wish to only capture traffic to and from particular IP hosts. To do this, use a tilde (~) symbol before the list of IP addresses. For example, to only capture packets to and from IP host 192.168.47.1, enter "~192.168.47.1" for this parameter.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
ana	0	anon	on, off	Enable Analyser
ana	0	maxdata	16 - 2000	Maximum packet capture size
ana	0	logsize	3 -180	Log Size
ana	0	l1on	on, off	Protocol Layers / Layer 1
ana	0	l2on	on, off	Protocol Layers / Layer 2
ana	0	l3on	on, off	Protocol Layers / Layer 3
ana	0	xoton	on, off	Protocol Layers / XOT
ana	0	ikeon	on, off	Enable IKE debug
ana	0	qmion	on, off	Enable QMI trace
ana	0	snaipon	on, off	Enable SNAIP trace
ana	0	lapdon	0 – 7 See below	ISDN Sources
ana	0	lapbon	0 – 7 See below	LAPB Links
ana	0	asyon	Bitmap See below	Serial Interfaces
ana	0	syon	Bitmap See below	Raw SYNC Sources
ana	0	discardson	on, off	IP Options / Trace discarded packets
ana	0	loopon	on, off	IP Options / Trace loopback packets
ana	0	ipfilt	Comma separated list	IP Packet Filters / TCP/UDP Ports
ana	0	ipprotfilt	Comma separated list	IP Packet Filters / IP Protocols
ana	0	ipaddfilt	Comma separated list	IP Packet Filters / IP Addresses
ana	0	discportfilt	Comma separated list	Discarded IP Packet Filters / TCP/UDP Ports
ana	0	discprotofilt	Comma	Discarded IP Packet Filters / IP

Entity	Instance	Parameter	Values	Equivalent Web Parameter
			separated list	Protocols
ana	0	discipaddfilt	Comma separated list	Discarded IP Packet Filters / IP Addresses
eth	n	ethanon	on, off	Ethernet Interfaces
eth	n	ipanon	on, off	IP Sources
ovpn	n	ipanon	on, off	IP Sources
ppp	n	ipanon	on, off	IP Sources
ppp	n	pppanon	on, off	PPP Interfaces
tun	n	ipanon	on, off	GRE IP Sources
tun	n	tunanon	on, off	GRE Tunnel Interfaces

Related CLI Commands not available via the Web Interface

Entity	Instance	Parameter	Values	Description
ana	0	fcon	on, off	Enable serial flow control tracing
ana	0	stopbufs	0 - 255	Stop analyser when number of free system buffers matches this value
ana	0	stopmsgs	0 - 255	Stop analyser when number of free system messages matches this value
ana	0	stopflood	0 - 1	Stop analyser when Ethernet flood protection is activated.
ana	0	lowbufcmd	Command String	Run this command when the number of free system buffers match “lowbuflvel”
ana	0	lowbuflev	Integer	Free system buffer threshold used by “lowbufcmd”.
ana	0	lowmsgcmd	Command String	Run this command when the number of free system messages match “lowmsglvel”
ana	0	lowmsglev	Integer	Free system message threshold used by “lowmsgcmd”.
ana	0	logdrive	String	Specifies an alternate file system drive on which to store the analyser trace. To use an external USB flash device, this should be set to “u:”. If the router has an internal SDIO flash device, it can be selected with “s:”.
ana	0	logfile	Filename	The file on the alternate drive to which the analyser trace will be stored.
ana	0	contfile	Filename	The file on the alternate drive to

Entity	Instance	Parameter	Values	Description
				which the analyser trace will be stored once the file indicated by “logfile” is reaches its max size as specified by “logsizek”.
ana	0	logsizek	Value in Kbytes	The maximum size in Kbytes of the file on the alternate drive. When set to 0, the file size is only limited by the flash device.

ISDN Sources

LAPD2	LAPD1	LAPD0	Value
OFF	OFF	OFF	0
OFF	OFF	ON	1
OFF	ON	OFF	2
OFF	ON	ON	3
ON	OFF	OFF	4
ON	OFF	ON	5
ON	ON	OFF	6
ON	ON	ON	7

LAPB Links

LAPD1	LAPD0	Value
OFF	OFF	0
OFF	ON	1
ON	OFF	2
ON	ON	3

Serial Interfaces

Interface	Value
Serial 0	1
Serial 1	2
Serial 2	4
Serial 3	8
Serial 4	16
Serial 5	32
Serial 6	64
Serial 7	128
Serial 8	256
Serial 9	512

Interface	Value
Serial 10	1024
Serial 11	2048
Serial 12	4096

To enable the analyser on multiple serial interfaces, add the appropriate values together. For example, to enable the analyser on serial interfaces 2 and 3, the value should 12 (4 + 8).

The number of Serial interfaces can vary on different depending on which hardware and software options are available.

Raw Sync Interfaces

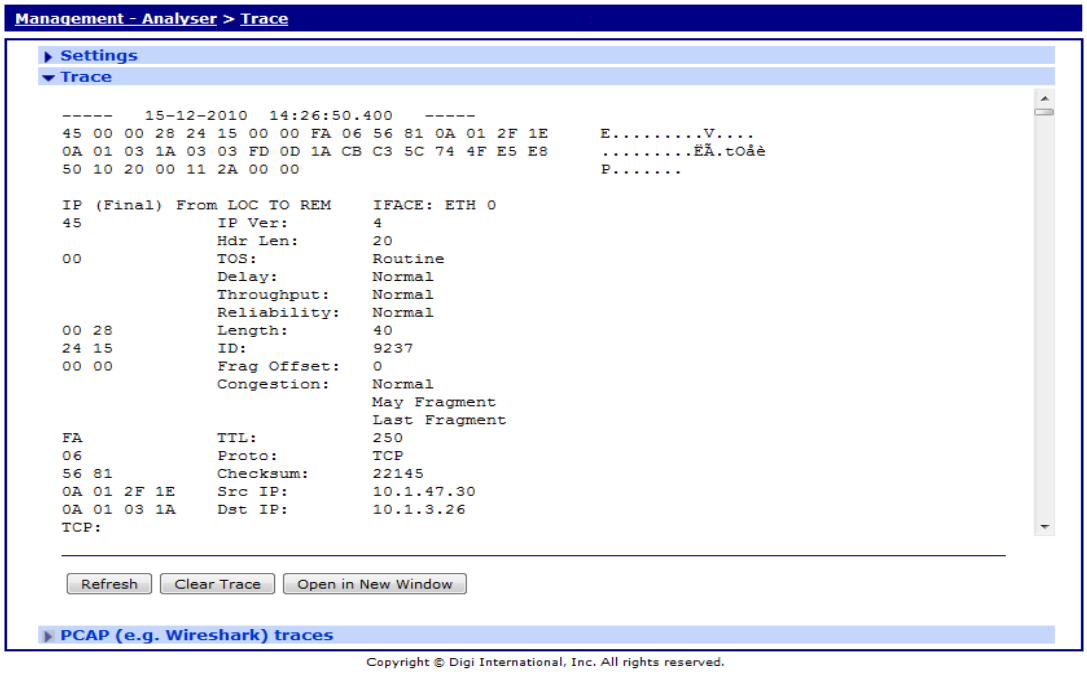
Interface	Value
ISDN D	1
ISDN B1	2
ISDN B2	4
Physical Port 0	8
Physical Port 1	16

To enable the analyser on multiple serial interfaces, add the appropriate values together. For example, to enable the analyser on Physical Ports 0 and 1, the value should 24 (8 + 16).

Trace

Management-Analyser > Trace

This displays the current analyser trace.


Management - Analyser > Trace
Settings
Trace
----- 15-12-2010 14:26:50.400 -----
45 00 00 28 24 15 00 00 FA 06 56 81 0A 01 2F 1E E.....V....
0A 01 03 1A 03 03 FD 0D 1A CB C3 5C 74 4F E5 E8 .....ËÃ.tOåè
50 10 20 00 11 2A 00 00 P.....
IP (Final) From LOC TO REM IFACE: ETH 0
45 IP Ver: 4
Hdr Len: 20
00 TOS: Routine
Delay: Normal
Throughput: Normal
Reliability: Normal
00 28 Length: 40
24 15 ID: 9237
00 00 Frag Offset: 0
Congestion: Normal
May Fragment
Last Fragment
FA TTL: 250
06 Proto: TCP
56 81 Checksum: 22145
0A 01 2F 1E Src IP: 10.1.47.30
0A 01 03 1A Dst IP: 10.1.3.26
TCP:
Refresh
Clear Trace
Open in New Window
PCAP (e.g. Wireshark) traces
Copyright © Digi International, Inc. All rights reserved.

Related CLI Commands

Command	Options	Description
type ana.txt		Displays the contents of the event log.
ana 0 anaclr		Clears the contents of the event log.

PCAP (e.g. Wireshark) traces

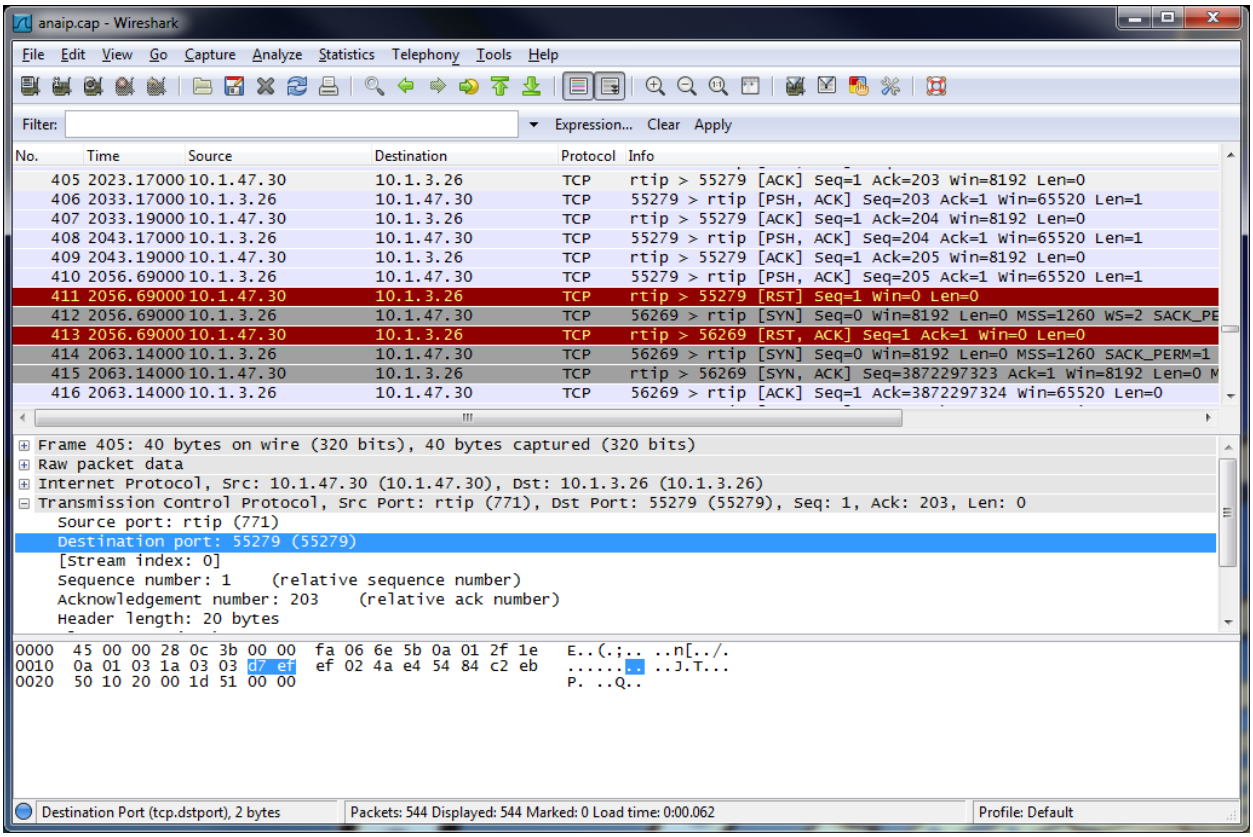
Management-Analyser> PCAP (e.g Wireshark) traces

The traffic captured by the Analyser is also available in PCAP format. This format can be read by a network protocol analyser such as Wireshark. This powerful feature gives a network engineer the ability to diagnose network protocol issues with relative ease.

There are several PCAP files which are available to download. Each file contains a different set of captured packets.

Option	PCAP File	Contents
IP	anaip.pcap	IP traffic captured from all enabled IP sources.
Ethernet	anaeth.pcap	Ethernet traffic captured from all enabled Ethernet sources.
PPP	anappp.pcap	PPP traffic captured from all enabled PPP sources.
Wi-Fi	anawifi.pcap	Wi-Fi traffic captured from the enabled Wi-Fi source.

Wireshark is free software and can be obtained from http://www.wireshark.org


anaip.cap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter: Expression... Clear Apply
No. Time Source Destination Protocol Info
405 2023.17000 10.1.47.30 10.1.3.26 TCP rtip > 55279 [ACK] Seq=1 Ack=203 Win=8192 Len=0
406 2033.17000 10.1.3.26 10.1.47.30 TCP 55279 > rtip [PSH, ACK] Seq=203 Ack=1 Win=65520 Len=1
407 2033.19000 10.1.47.30 10.1.3.26 TCP rtip > 55279 [ACK] Seq=1 Ack=204 Win=8192 Len=0
408 2043.17000 10.1.3.26 10.1.47.30 TCP 55279 > rtip [PSH, ACK] Seq=204 Ack=1 Win=65520 Len=1
409 2043.19000 10.1.47.30 10.1.3.26 TCP rtip > 55279 [ACK] Seq=1 Ack=205 Win=8192 Len=0
410 2056.69000 10.1.3.26 10.1.47.30 TCP 55279 > rtip [PSH, ACK] Seq=205 Ack=1 Win=65520 Len=1
411 2056.69000 10.1.47.30 10.1.3.26 TCP rtip > 55279 [RST] Seq=1 Win=0 Len=0
412 2056.69000 10.1.3.26 10.1.47.30 TCP 56269 > rtip [SYN] Seq=0 Win=8192 Len=0 MSS=1260 WS=2 SACK_PE
413 2056.69000 10.1.47.30 10.1.3.26 TCP rtip > 56269 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
414 2063.14000 10.1.3.26 10.1.47.30 TCP 56269 > rtip [SYN] Seq=0 Win=8192 Len=0 MSS=1260 SACK_PERM=1
415 2063.14000 10.1.47.30 10.1.3.26 TCP rtip > 56269 [SYN, ACK] Seq=3872297323 Ack=1 Win=8192 Len=0
416 2063.14000 10.1.3.26 10.1.47.30 TCP 56269 > rtip [ACK] Seq=1 Ack=3872297324 Win=65520 Len=0
Frame 405: 40 bytes on wire (320 bits), 40 bytes captured (320 bits)
Raw packet data
Internet Protocol, Src: 10.1.47.30 (10.1.47.30), Dst: 10.1.3.26 (10.1.3.26)
Transmission Control Protocol, Src Port: rtip (771), Dst Port: 55279 (55279), Seq: 1, Ack: 203, Len: 0
Source port: rtip (771)
Destination port: 55279 (55279)
[Stream index: 0]
Sequence number: 1 (relative sequence number)
Acknowledgement number: 203 (relative ack number)
Header length: 20 bytes
0000 45 00 00 28 0c 3b 00 00 fa 06 6e 5b 0a 01 2f 1e E..(.;.. ..n[../.
0010 0a 01 03 1a 03 03 d7 ef ef 02 4a e4 54 84 c2 eb ....J.T...
0020 50 10 20 00 1d 51 00 00 P. ..Q..
Destination Port (tcp.dstport), 2 bytes
Packets: 544 Displayed: 544 Marked: 0 Load time: 0:00.062
Profile: Default

Top Talkers Management

The router can be configured to monitor the data being transmitted and received on the various interfaces. It is able to report which IP hosts are generating the most traffic over a period of one minute and 30 minutes.

Top Talkers also allows you to block particular IP traffic flows to stop them from using bandwidth. The ***Management-Top Talkers*** page has the following menu options:

- Settings
- Trace

Settings

Management-Top Talkers > Settings

Ethernet Interfaces
The checkboxes shown under this heading are used to select the Ethernet interfaces that Top Talkers will monitor.

PPP Interfaces
The checkboxes shown under this heading are used to select the PPP interfaces that Top Talkers will monitor.

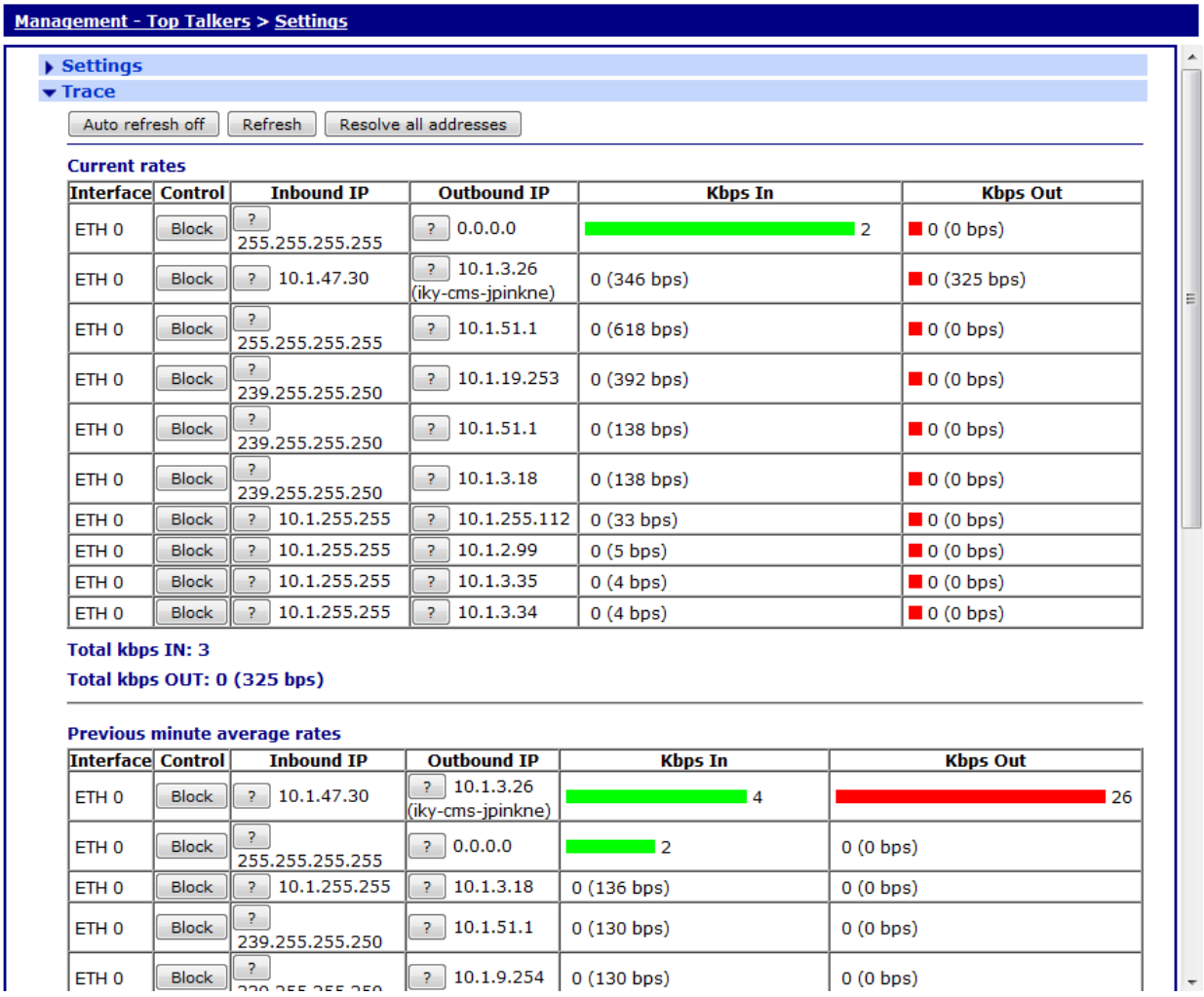
Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
eth	n	ttalker	on | off	Ethernet Interfaces
ppp	n	ttalker	on | off	PPP Interfaces

Trace

Management-Top Talkers > Trace

This displays the current top talkers trace.


Management - Top Talkers > Settings
Settings
Trace
Auto refresh off
Refresh
Resolve all addresses
Current rates
Interface | Control | Inbound IP | Outbound IP | Kbps In | Kbps Out
ETH 0 | Block | ? 255.255.255.255 | ? 0.0.0.0 | 2 | 0 (0 bps)
ETH 0 | Block | ? 10.1.47.30 | ? 10.1.3.26 (iky-cms-jpinkne) | 0 (346 bps) | 0 (325 bps)
ETH 0 | Block | ? 255.255.255.255 | ? 10.1.51.1 | 0 (618 bps) | 0 (0 bps)
ETH 0 | Block | ? 239.255.255.250 | ? 10.1.19.253 | 0 (392 bps) | 0 (0 bps)
ETH 0 | Block | ? 239.255.255.250 | ? 10.1.51.1 | 0 (138 bps) | 0 (0 bps)
ETH 0 | Block | ? 239.255.255.250 | ? 10.1.3.18 | 0 (138 bps) | 0 (0 bps)
ETH 0 | Block | ? 10.1.255.255 | ? 10.1.255.112 | 0 (33 bps) | 0 (0 bps)
ETH 0 | Block | ? 10.1.255.255 | ? 10.1.2.99 | 0 (5 bps) | 0 (0 bps)
ETH 0 | Block | ? 10.1.255.255 | ? 10.1.3.35 | 0 (4 bps) | 0 (0 bps)
ETH 0 | Block | ? 10.1.255.255 | ? 10.1.3.34 | 0 (4 bps) | 0 (0 bps)
Total kbps IN: 3
Total kbps OUT: 0 (325 bps)
Previous minute average rates
Interface | Control | Inbound IP | Outbound IP | Kbps In | Kbps Out
ETH 0 | Block | ? 10.1.47.30 | ? 10.1.3.26 (iky-cms-jpinkne) | 4 | 26
ETH 0 | Block | ? 255.255.255.255 | ? 0.0.0.0 | 2 | 0 (0 bps)
ETH 0 | Block | ? 10.1.255.255 | ? 10.1.3.18 | 0 (136 bps) | 0 (0 bps)
ETH 0 | Block | ? 239.255.255.250 | ? 10.1.51.1 | 0 (130 bps) | 0 (0 bps)
ETH 0 | Block | ? | ? 10.1.9.254 | 0 (130 bps) | 0 (0 bps)

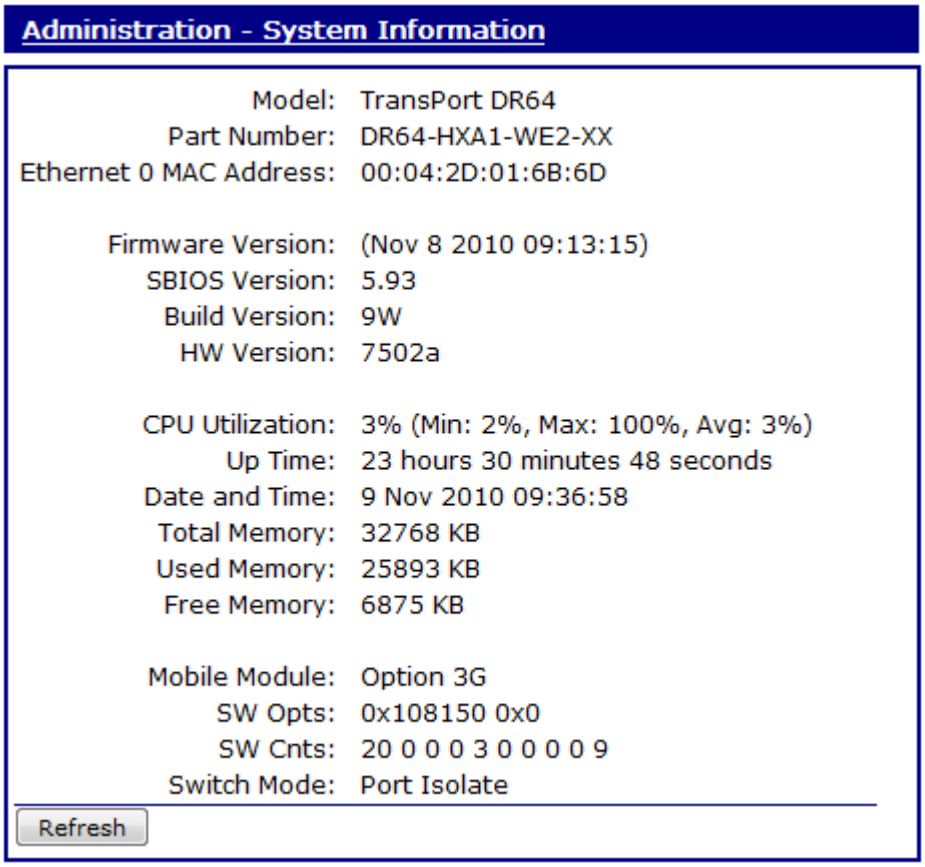
Administration Page

The ***Administration*** page has following options:

- System Information
- File Management
- X.509 Certificate Management
- Backup/ Restore
- Update Firmware
- Factory Default Settings
- Execute a command
- Save configuration
- Reboot

System Information Administration

The ***Administration – System Information*** page gives an overview of the status of the router.


Administration - System Information
Model: TransPort DR64
Part Number: DR64-HXA1-WE2-XX
Ethernet 0 MAC Address: 00:04:2D:01:6B:6D
Firmware Version: (Nov 8 2010 09:13:15)
SBIOS Version: 5.93
Build Version: 9W
HW Version: 7502a
CPU Utilization: 3% (Min: 2%, Max: 100%, Avg: 3%)
Up Time: 23 hours 30 minutes 48 seconds
Date and Time: 9 Nov 2010 09:36:58
Total Memory: 32768 KB
Used Memory: 25893 KB
Free Memory: 6875 KB
Mobile Module: Option 3G
SW Opts: 0x108150 0x0
SW Cnts: 20 0 0 0 3 0 0 0 0 9
Switch Mode: Port Isolate
Refresh

Model
This describes the model of the router.

Part Number
This describes the Digi part number of the router.

Ethernet 0 MAC Address
This describes the MAC address of the Ethernet 0 interface.

Firmware Version
This describes the firmware version that is currently running on the router.

SBIOS Version
This describes the SBIOS firmware version that is currently running on the router.

Build Version
This describes the build configuration of the firmware that is currently running on the router.

HW Version
This describes the hardware version on the router. Please note this item may be blank.

CPU Utilization
This describes the current and historical CPU utilization since the router booted up.

Up Time
This describes the amount of time since the router booted up.

Date and Time
This describes the current date and time on the router.

Total Memory
This describes the total amount of RAM that is fitted on the router.

Used Memory
This describes the amount of RAM that is currently being used on the router.

Free Memory
This describes the amount of RAM that is currently free on the router.

Mobile Module
This describes which mobile module is fitted on the router.

SW Opts
This describes which firmware options have been enabled on the router.

SW Cnts
This describes some configuration parameters that are used by firmware.

Switch Mode
This describes the current setting of the Ethernet switch on routers with multiple Ethernet interfaces. It can be either “Hub” or “Port Isolate”.

Related CLI Commands

Command	Options	Equivalent Web Parameter
ati5	n/a	Model Firmware Version SBIOS Version Build Version Mobile Module SW Opts
hw	n/a	Part Number Ethernet 0 MAC Address HW Version
cpu	n/a	CPU Utilization
uptime	n/a	Up Time
time	n/a	Date and Time
mem	n/a	Total Memory Used Memory Free Memory

File Management Administration

The ***Administration – File Management*** page has the following menu options:

- FLASH Directory
- WEB Directory
- File Editor

FLASH Directory

Administration – File Management > FLASH Directory

This page displays the contents of the router's flash file system.

The unit has its own FLASH memory fling system that uses DOS-like filenames of up to 12 characters long (8 characters followed by the "." separator and a 3-character extension). The filing system is used to store the system software, Web pages, configuration information and statistics in a single root directory.

Sub-directories are not supported and a maximum of 80 - 300 files (depending on the product) can be stored (including system files), providing there is sufficient memory remaining. New files can be uploaded into the unit from a local terminal or from a remote system over the WAN connection. Existing files can be renamed or deleted using DOS-like commands.

Although the filing system will only store a limited number of files, all those associated with the built-in Web interface are stored in a single file with the .WEB extension and extracted as required.

The Administration - File Management > FLASH Directory web page displays a listing of files held on the FLASH file system. These files appear as hyperlinks which can be downloaded and displayed in the web browser as long an appropriate viewer is installed and a file association with the viewer has been made.

The directory listing of files on the FLASH directory also shows the file size, the access of rw (read write) or ro (read only) and the date the file was last modified.

Below the file list is a summary of the FLASH file system, this includes the number of files, FLASH free and FLASH used.

Action

Action checkbox is used to select each read/write file for deletion.

File
This is the name of the file in the flash file system.

Size (bytes)

This is the size of the file in bytes. This is not a fixed value. When downloaded, the size of the downloaded file will be different.

Access
This is the access settings for the file.

rw	Read / Write access
ro	Read Only access

Last Modified

The date and time of when the file was last modified.

Delete Selected Files

This button is used to delete the selected files.


FLASH Directory
Action File Name Size Access Last Modified
user <DIR>
direct 52224 bytes ro 12:56:14, 30 Mar 2011
sbios 262144 bytes ro 23:07:49, 22 Jan 2000
mirror 52224 bytes ro 12:56:14, 30 Mar 2011
privpy.enc 61524 bytes rw 23:05:40, 22 Jan 2000
CAcert.cer 1371 bytes rw 12:56:14, 30 Mar 2011
x3prof 4096 bytes rw 12:57:51, 30 Mar 2011
sregs.dat 4096 bytes rw 00:11:37, 01 Jan 2000
config.fac 8395 bytes ro 12:56:14, 30 Mar 2011
LOGCODES.TXT 20008 bytes rw 23:05:37, 22 Jan 2000
passcng.py 836 bytes rw 14:44:23, 05 Apr 2011
sregs.fac 4096 bytes ro 12:56:14, 30 Mar 2011
python.zip 1631612 bytes rw 23:06:04, 22 Jan 2000
cert01.pem 3285 bytes rw 12:56:14, 30 Mar 2011
image4.c1 215801 bytes rw 23:07:32, 22 Jan 2000
privrsa.pem 887 bytes rw 12:56:14, 30 Mar 2011
config.da0 8520 bytes rw 22:51:45, 07 Jan 2000
manual.sb 26826 bytes rw 12:56:14, 30 Mar 2011
activate.sb 33685 bytes rw 12:56:14, 30 Mar 2011
gobiact.sb 22519 bytes rw 12:56:14, 30 Mar 2011
prlupdate.sb 31523 bytes rw 12:56:14, 30 Mar 2011
provision.sb 19501 bytes rw 12:56:14, 30 Mar 2011
pppfcs.sb 7784 bytes rw 12:56:14, 30 Mar 2011
queryimsi.sb 10661 bytes rw 12:56:14, 30 Mar 2011
wizards.zip 276265 bytes rw 23:15:44, 22 Jan 2000
51 Files, Flash Used: 8375467 Bytes, Flash Free: 57753600 Bytes
Delete selected files

Related CLI Commands

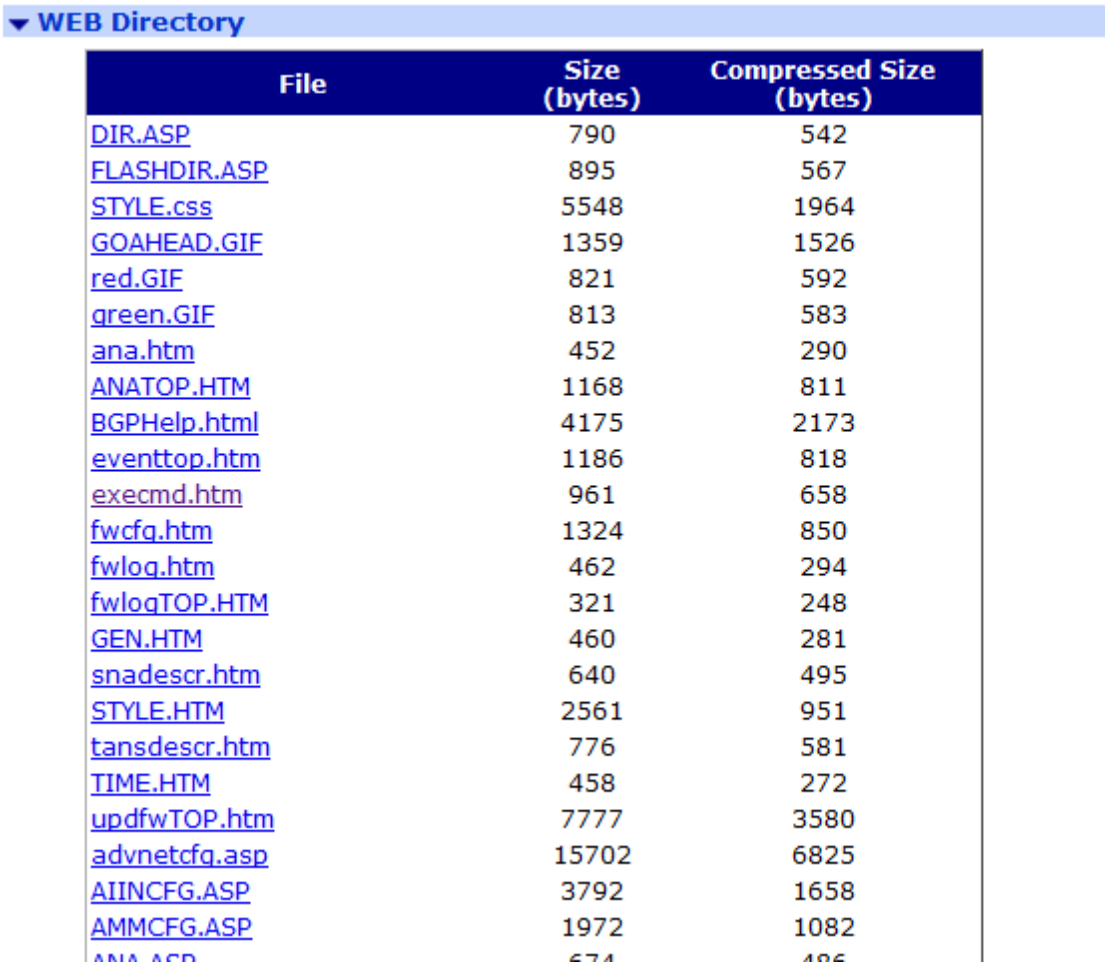
Command	Options	Equivalent Web Parameter
dir		Displays the entire contents of the router's flash file system.
dir	<filter>	Displays a filtered view of the router's flash file system. The filter can contain wildcards using the *. e.g. *dir *.pem* to display all the files ending in ".pem".
dir	u:	Displays the contents of an USB flash stick if inserted into the USB port of the router.

WEB Directory

Administration – File Management > WEB Directory

The WEB directory contains a list of the files held within the active web file. The web file is shown on the FLASH file system as a single file, this file is compressed and holds approximately 300 files.

Direct access to these files by an engineer is not normally required.



File
The name of the file in web file.

Size (Bytes)
The size of the file in bytes.

Compressed Size (Bytes)
The compressed size of the file in bytes.

File Editor

The file editor allows the user to edit text files on the router.



Filename
The name of the file to edit.
It is possible to create a new file by typing in the filename and clicking on the “Save File” button.

Load File
Load the file specified in “Filename” into the editor box.

Save File
Save the file to the flash file system.

X.509 Certificate Management Administration

The X.509 Certificate Management pages are for loading and managing X.509 certificates and public/private host key pairs that are public key infrastructure (PKI) based security.

The ***Administration -> X.509 Certificate Management*** Page has the following menu options:

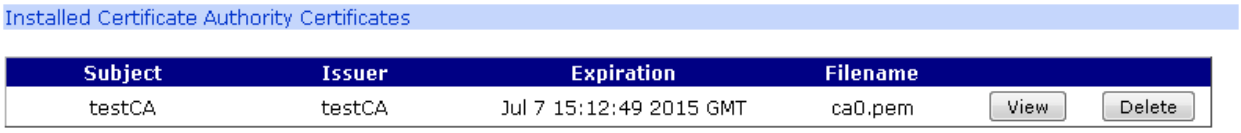
- Certificate Authorities (CAs)
- IPsec/SSH/HTTPS Certificates
- Key Generation

Certificate Authorities (CAs)

Administration -> X.509 Certificate Management> Certificate Authority (CA)

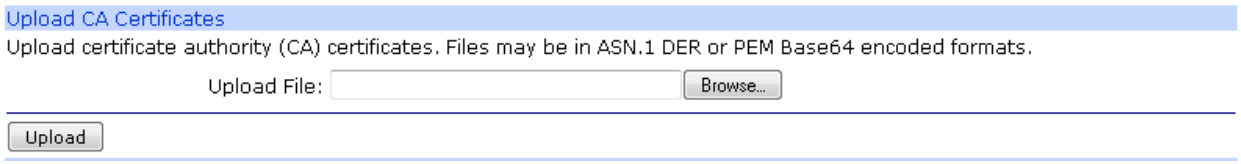
A certificate authority (CA) is a trusted third party which issues digital certificates for use by other parties.
Digital certificates issued by the CA contain a public key. The certificate also contains information about the individual or organization to which the public key belongs.
A CA verifies digital certificate applicants' credentials. The CA certificate allows verification of digital certificates and the information contained therein, issued by that CA.

Installed Certificate Authority Certificates



This table lists the current CA certificates that have been installed onto the router. It is possible to view the contents of each certificate using the “View” button.

Upload CA Certificates



CA Certificates can be uploaded from a host PC onto the router using the “Browse” and “Upload” buttons.

Obtain CA certificates from a SCEP Server

The Simple Certificate Enrolment Protocol (SCEP) allows the user to request and enrol CA certificates from a CA server.

The CA certificate files will automatically stored with the name CA<n>.pem where n increments with each certificate.

SCEP Server IP address
The IP address of the SCEP server / CA server.

Port
The port on which SCEP server is listening. If the port is 0, the default port of 80 will be used.

Path
The path on the server to the SCEP application. The path can either be entered manually if known or select from cgi-bin or Microsoft SCEP from the drop-down list.

Application
The SCEP application running on the server.

CA identifier
The identifier for the CA server. The CA identifier to use to identify a particular CA when multiple CAs might be running on the server.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
scep	0	host	IP Address	SCEP Server IP address
scep	0	port	0 - 65535	Port
scep	0	path	String	Path
scep	0	app	String	Application
scep	0	caident	String	CA Identifier

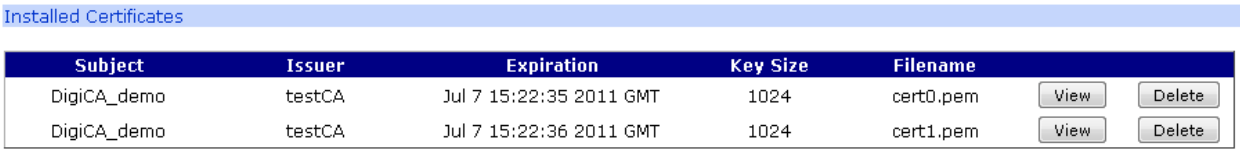
IPsec / SSH / HTTPS Certificates

Administration -> X.509 Certificate Management> IPsec / SSH / HTTPS Certificates

This page contains fields that required when sending a certificate request to a Certificate Authority (CA). This information forms part of the certificate request, and thus part of the signed public key certificate.

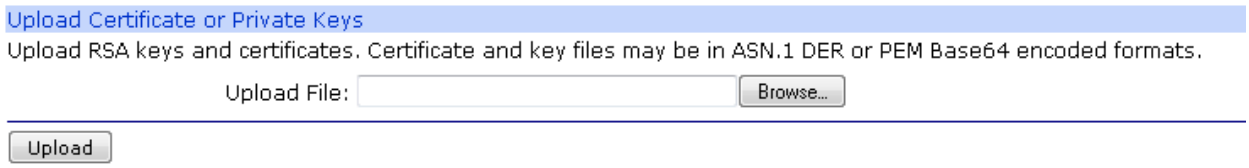
The router can use certificates to establish IPsec tunnels with other routers and support SSH and HTTPS connections. For more information on using certificates with the router, please refer to the Application Note “How to configure an IPSEC VPN tunnel between two Digi Routers using Certificates and SCEP”, which are available from the Digi web site.

Installed Certificates



This table lists the current certificates that have been installed onto the router. It is possible to view the contents of each certificate using the “View” button.

Upload Certificate or Private Keys



Certificates and private key files can be uploaded from a host PC onto the router using the “Browse” and “Upload” buttons.

Enrolment

The following parameters allow the user to create a certificate request, enroll them and to install the certificates on the router.

SCEP Server IP address
The IP address of the SCEP server / CA server.

Port
The port on which SCEP server is listening. If the port is 0, the default port of 80 will be used.

Path
The path on the server to the SCEP application. You can either enter your own path or select from cgi-bin or Microsoft SCEP from the drop-down list.

Application
The SCEP application running on the server.

CA identifier
The identifier for the CA server. The CA identifier to use to identify a particular CA when multiple CAs might be running on the server.

CA certificate
The filename of the CA certificate.

CA encryption certificate
Sometimes when you get a CA certificate, a CA encryption certificate is installed on the router at the same time. You can identify a CA encryption certificate by looking at the X.509 Key Usage section in the certificate. It should say something like the following

```
X509v3 Key Usage: critical
    Key Encipherment, Data Encipherment
```

If a CA encryption certificate has been installed by the CA you wish to use for the certificate request, the CA encryption certificate should be entered.

If no CA encryption certificate has been installed for the CA, leave this file blank.

CA signature certificate
Sometimes when you get a CA certificate, a CA signature certificate is installed on the router at the same time. You can identify a CA signature certificate by looking at the X.509 Key Usage section in the certificate. It should say something like the following

```
X509v3 Key Usage: critical
    Digital Signature, Non Repudiation
```

If a CA signature certificate has been installed by the CA you wish to use for the certificate request, the CA signature certificate should be entered.
If no CA signature certificate has been installed for the CA, leave this file blank.

RSA Private key
This parameter allows you to select between using an existing private key and generating a one for each certificate request.

Private key filename
The filename of the private key file to use.

Enrolment Password

Before you can create a certificate request you must first obtain a challenge password from the Certificate Authority Server. This password is generally obtained from the SCEP CA server by way of a WEB server or a phone call to the CA Server Administrator. For the Microsoft® SCEP server, you browse to a web interface. If the server requires a challenge password, it will be displayed on the page along with the CA certificate fingerprint.
This challenge password is usually only valid once and for a short period of time, in this case 60 minutes, meaning that a certificate request must be created after retrieving the challenge password.

Common Name (CN)
A name for the router. This parameter is important as the common name will be used as the router's ID for IKE negotiations.

Country Code (C)
The two character county code of where the router is located. A list of valid country codes can be found at http://www.iso.org/iso/english_country_names_and_code_elements.

State or Province (ST)
The state, county or province of where the router is located.

Locality (L)
The town or city of where the router is located.

Organisation (O)
The company to whom the router belongs to.

Organisational Unit (OU)
The company department maintaining the router.

E-mail
An appropriate email address of a contact for the router.

Unstructured Name
This parameter is optional. It can contain some descriptive to help identify the certificate.

Digest Algorithm
The digest algorithm used (MD5 or SHA1) when signed the certificate request.

Ignore NONCE in SCEP response
The parameter instructs the router to ignore the NONCE field in the SCEP response. The NONCE is primarily used to prevent replay attacks.

Related CLI Commands

Entity	Instance	Parameter	Values	Equivalent Web Parameter
scep	0	host	IP Address	SCEP Server IP address
scep	0	port	0 - 65535	Port
scep	0	path	String	Path
scep	0	app	String	Application
scep	0	caident	String	CA Identifier
scep	0	cafile	Filename	CA certificate
scep	0	caencfile	Filename	CA encryption certificate
scep	0	casigfile	Filename	CA signature certificate
creq	0	challenge_pwd	String	Enrolment Password

Entity	Instance	Parameter	Values	Equivalent Web Parameter
creq	0	commonname	String	Common Name (CN)
creq	0	country	String	Country Code (C)
creq	0	state	String	State or Province (ST)
creq	0	locality	String	Locality (L)
creq	0	orgname	String	Organisation (O)
creq	0	org_unit	String	Organisational Unit (OU)
creq	0	email	Email Address	E-Mail
creq	0	unstructname	String	Unstructured Name
creq	0	digest	MD5 or SHA1	Digest Algorithm

The **creq** command can also be used to generate the certificate request using the configured parameters. If the private key does not already exist and appropriate parameters are entered, the key will be generated at the same time.

To generate a certificate request, enter the command:

creq new -k<priv key file> -o<cert request file>

To generate a private key and a certificate request, enter the command:

creq new –b<priv key length> -k<priv key file> -o<cert req file>

For example, to generate a certificate request file called “request.pem” from a private key called “priv001.pem”, enter:

creq new -kpriv001.pem -o request.pem

To generate a 512 bit private key called “private.pem”, and generate a certificate request called “certreq.pem” using that file, enter:

creq new -b512 -kprivate.pem -ocertreq.pem

Key Generation

Administration -> X.509 Certificate Management> Key Generation

This page allows you to generate a private key. A private key must be created before a certificate can be requested as it is used in the request.

Key filename

Enter a name for the private key (the filename must be prefixed with “priv” and have a “.pem” extension).

Key size

The size of the private key in bits. The key size can be one of the following

- 384
- 512
- 768
- 1024
- 1536
- 2048

The larger the key, the more secure the connection, but also the larger the key, the slower the connection.

Save in SSHv1 format

If this checkbox is checked the private key will be generated in SSH version 1 format. If it is cleared the private key will be generated in SSH version 2 format.

Related CLI Commands

The **genkey** command can be used to generate a private key file.

To generate a private key, enter the command

genkey 0 <keysize> <filename> <-ssh1>

where

<*keysize*> is the size of the key in bits.

<*filename*> is the name of the private key file.

<*-ssh1*> is optional, and will generate the private key file in SSH version 1 format.

Note: IPsec requires SSH version 2 private keys.

For example, to generate a 1024 bit SSH version 2 key called privkey.pem, enter:

genkey 1024 privkey.pem

You will see the following output:

OK

Starting 1024 bit key generation. Please wait. This may take some time...

Key generated, saving to FLASH file privkey.pem

Closing file

Private key file created

All tasks completed

Private key files - Splitting Certificates

For increased security there is the option of splitting the private key file between the Digi flash and an USB memory stick. Once a private key has been split and stored in 2 parts, the USB memory stick must be present for any successful IKE negotiations that involve the private key. As the USB memory stick only contains a part of the private key, it cannot be used in another unit.

The command to split a private key is:

privsplit <certificate filename>

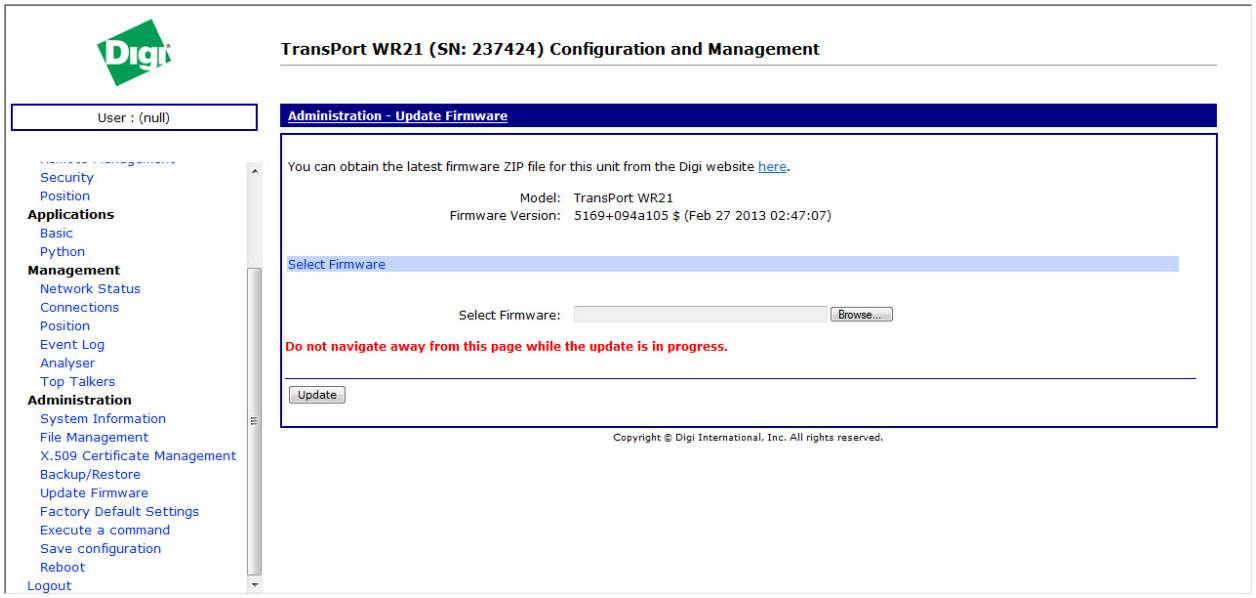
Update Firmware

The ***Administration –Update Firmware*** page allows the user to update the router's firmware. The router will download a zip file onto the router, uncompress it, validate each file within the zip file and then update the files in its flash file system.

The zip file containing the latest firmware version is available from the Digi website (http://transport.digi.com/digi/firmware/ftp/). The zip file should be downloaded to your PC before starting the firmware update.

Note: It is important that you DO NOT NAVIGATE AWAY from the Update Firmware page whilst an update is in progress as it can cause the update to abort prematurely.

It is also important that you DO NOT REMOVE THE POWER from the router whilst an update is in progress as it can corrupt the router's flash file system and might leave the router unable to boot up.



Model

This indicates which model this router is.

Firmware Version

This indicates the current firmware version running on the router.

Select Firmware

Select the zip file on your PC containing the firmware version to you wish to update to.

Once the firmware update is complete, the router has to be rebooted before the new firmware version can run.

Factory Default Settings

The ***Administration – Factory Default Settings*** page allows you to reset the router's configuration back to the factory defaults.

The router must be rebooted before the configuration changes take effect.

Keep network settings
Selecting this option will mean that certain network settings will be preserved and not reverted back to the factory defaults.

The network settings that are preserved are

- Ethernet 0 IP address
- Ethernet 0 Mask
- Ethernet 0 Gateway
- Ethernet 0 DHCP Client
- Ethernet 0 DNS Server
- Default Route 0 Interface
- PPP 1 Username
- PPP 1 Password
- PPP 3 Username
- PPP 3 Password
- Mobile APN
- Mobile SIM PIN

Restore
Clicking this button initiates a factory reset of the router.

Related CLI Commands

The router's configuration can be reset back to the factory defaults using the following commands

del pwds.da0

copy config.fac config.da0
This assumes that you are using configuration profile 0. If configuration profile 1 is being used, then the .da1 suffix should be used instead of .da0.
Please note that using these commands does not preserve any network settings.

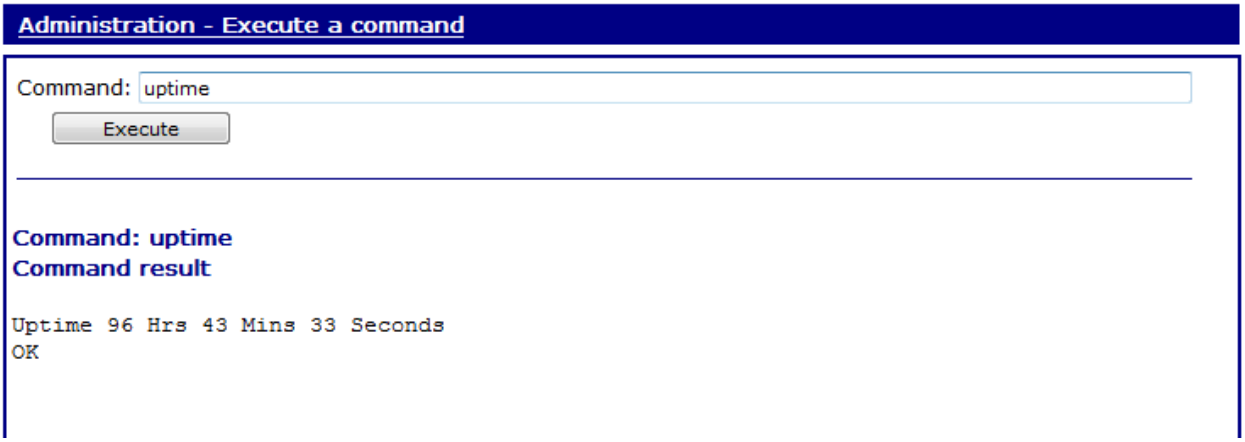
Reset using the hardware Reset button
There is a reset button on the underside of most routers, holding this button in for 5 seconds will perform a factory reset on the router. When the reset is initiated in this manner, the LEDs on the front of the router will flash to indicate a reset is in progress, the router will automatically reboot once the procedure is complete. Do not remove the power whilst the router is running this reset procedure. Using this method will not preserve any settings.

The CLI command to disable the reset button is "*cmd 0 pbreset off*"

To re-enable the reset button functionality "*cmd 0 pbreset on*"

Execute a command

The ***Administration –Execute a Command*** page allows CLI commands to be entered via the web browser. Almost all of the CLI commands detailed in this reference guide can be entered via this page. The corresponding output will be shown when the 'Execute' button is pressed.



Save configuration

Administration – Save configuration

Once you have configured the router, your chosen settings must be saved to non-volatile memory to avoid losing them when the power is removed.

Save current configuration to Config n
This parameter can be used to set the configuration file to which the current configuration will be saved when the "Save" button is clicked. There are 2 options, profile 0 and profile 1. The default power up profile is profile 0.

The configuration profile that is used when the router powers up is indicated in the selection box.

Save all configuration
The "Save All" button saves the router's entire configuration.

- The current configuration parameters to config.da0 or config.da1 file**
- The ciphered versions of the passwords to the pwds.da0 or pwds.da1 file**
- The Firewall configuration to the fw.txt file
- The serial port configuration to profile 0 of the sregs.dat file
- The PAD parameters on all the PADs to profile 0 of the x3prof file

Related CLI Commands

Parameter	Options	Equivalent Web Parameter
config	save	Save current configuration to Config n
saveall	n/a	Save all configuration

** The default power up profile is profile 0. *.da0 = profile 0, *.da1 = profile 1.

Reboot

The ***Administration*** - ***Reboot*** page is used to reboot the router immediately or at a scheduled time.

A reboot will be performed after any FLASH write operations have been completed. Also, one second each is allowed for the following operations to be completed before reboot will take place:

- IPSec SA delete notifications have been created and sent
- TCP sockets have been closed
- PPP interfaces have been disconnected

Immediately
Selecting this option will cause the router to reboot after a few seconds. The router will cleanly terminate any TCP and VPN connections before rebooting.

In h hrs m mins s secs
Selecting this option will cause a reboot to be scheduled after the configured period of time. A scheduled reboot can be cancelled by clicking the “Cancel” button.

Related CLI Commands

Command	Options	Equivalent Web Parameter
reboot	n/a	Immediately
reboot	0 – 86400	In h hrs m mins s secs. This CLI value is entered in minutes only.
reboot	cancel	Cancel reboot

Logout

Clicking the Logout link in the menu on the left will log out the current user and return to the login page

Filing system & system files

The dir command described below is used to display a list of the currently stored files. A typical file directory will include the following files:

Filename	Description
ana.txt	Pseudo file for Protocol Analyser output
config.da0	Data file containing Config.0 settings
direct	File directory
eventlog.txt	Pseudo file for Event Log output
fw.txt	Firewall script file
fwstat.txt	Firewall script status file
image	Main system image
*.web	File containing compressed Web pages for your model
logcodes.txt	Text file containing Event Log config. info.
pwds.da0	File containing obfuscated passwords
sbios	TransPort BIOS and bootloader
sregs.dat	Data file containing AT command & S register settings
x3prof	X.25 PAD profile parameters

Once you have configured the unit, your chosen settings must be saved to non-volatile memory to avoid losing them when the power is removed. Application command settings are stored in one of two “CONFIG” files. AT command and S register settings are stored in one file call “SREGS.DAT”.

Config Files

Most configuration information is stored in one of two files called “CONFIG.DA0” and “CONFIG.DA1”. This allows two different sets of configuration information to be stored using the Save option in the directory tree at the left of the web interface, or by using the config command from the command line.

The **Save All** button will save:

File name	Configuration held in file
config.da0	Main configuration parameters
pwds.da0	Encrypted passwords
fw.txt	Firewall rules
sregs.dat	Serial port S registers
x3prof	X.25 PAD profiles

You may select which of the two config files is loaded when the unit is powered-up or rebooted by setting the parameter ***Configuration - System > General > Miscellaneous > Use Config n when the router powers up*** as required (or by using the *config n powerup* CLI command).

Note:
The CONFIG files only contain details of settings that have been changed from the default values.

SREGS.DAT

A combined set of AT command and S register settings are referred to as a "profile". Two such profiles (0 and 1) may be stored for each ASY port in a file called "SREGS.DAT" using the **Save Profile** button on the relevant ***Configuration - Network > Interfaces > Serial > Serial Port n*** web page, or by using the AT&W command.

It is important to remember that saving the settings for one ASY port does not save the settings for the other ports so the settings for each port must be saved individually.

For each ASY port, the profile to be loaded at reboot or power-up is specified in the **Power-up Profile** setting on the relevant ***Configuration - Network > Interfaces > Serial > Serial Port 0*** web page (or by using AT&Y command).

A profile for a particular ASY port may also be loaded to take immediate effect by using the **Load Profile** button on the ASY port's web page, or by using the ATZ command.

PWDS.DA0

As of firmware version 4981, the encrypted forms of passwords entered into the configuration are stored in a separate file named pwds.da0. This file can only be accessed by users with Super level privileges. The file can be read with the type command, e.g. *type pwds.da0*

The pwds.da0 file is only created when a password is changed from default and the configuration is saved. The encrypted versions of the default passwords are then removed from the config.da0 file and the new pwds.da0 is created and used instead.

If the pwds.da0 file is deleted all remote access to the router that requires authentication will fail, a serial cable connection will be required to re-configure passwords to gain access to the router. If both the pwds.da0 file exists and the config.da0 contains passwords also, the passwords in the config.da0 take precedence and will over write the passwords in the pwds.da0 when a save command is issued.

Filing System Commands

COPY Copy File

The *copy* command is used to make a copy of a file. The format is:

copy <filename> <newfilename>

where *<filename>* is the name of an existing file and *<newfilename>* is the name of the new copy that will be created.

DEL Delete File

The *del* command is used to delete files from the filing system. The format is:

del <filename>

where *<filename>* is the name of an existing file.

You can also use wild cards in the filename in order to delete several files at once. The * character can represent one or more characters in the filename.
For example, *del fw*.txt* will delete fw.txt and fwstat.txt. The *del* command returns *OK* if files have been deleted, or *ERROR* if no matching files have been found.

DIR List File Directory

The dir command is used to display the file directory. For example:

```
dir
      direct    60720 ro   11:30:41, 31 Jan 2011 CRC  ???
       sbios   524288 ro   11:30:43, 31 Jan 2011 CRC 6ba8
      mirror    60720 ro   11:30:41, 31 Jan 2011 CRC  ???
       image  4300995 rw   15:22:23, 31 Jan 2011 CRC ab19
   sregs.dat     4096 rw   11:30:41, 31 Jan 2011 CRC 08b2
      x3prof     4096 rw   11:30:41, 31 Jan 2011 CRC bb5f
  CAcert.cer     1371 rw   11:30:41, 31 Jan 2011 CRC 6764
```

Each line shows the file name and extension (if any), the file size (in bytes), the read/write status (ro = read only, rw = read/write), the time/date of creation and the CRC value.

Note:
File write operations are carried out as a background task and can be relatively slow due to the constraints of FLASH memory. As a result, the file directory may only be updated several seconds after a particular file operation has been carried out.

You can also use wildcards with the dir command in order to narrow your search. The * character can represent one or more characters in the filename. For example, dir fw*.txt will list only the fw.txt and fwstat.txt files (if they are present on the TransPort).

FLOCK Lock Files

The *flock* command prevents any further writing to the FLASH memory. This means that no files can be written to, added to or deleted from the filing system.

FUNLOCK Unlock Files

The *funlock* command unlocks the FLASH memory if it had been locked using the flock command. Files can then be added, deleted or copied to the filing system.

MOVE Move File

The *move* command is used to replace one file with another whilst retaining the original filename. The format is:

move <fromfile> <tofile>

For example, the command:

move fw-temp.txt fw.txt

will delete the file called “fw.txt” and then rename the file called “fw-temp.txt” as “fw.txt”.

REN Rename File

The *ren* command is used to rename files in the filing system. The format is:
`ren <oldfilename> <newfilename>`

SCAN / SCANR Scan File System

The *scan* command performs a diagnostic check on the file system and reports any errors that are found. For example:

```
scan
Please wait...
      direct ....ok
       sbios ....ok
      mirror ....ok
       image ....ok, data ok
   sregs.dat ....ok
      x3prof ....ok
  CAcert.cer ....ok
```

The scanning process may take several seconds so you should not enter any other commands until the results are listed.

The *scanr* command works in a similar fashion, except that it will return ERROR if any file is in error. This is useful when used with scripts that can look for the ERROR failure result.

TYPE Display Text File

The *type* command is used to display the contents of a text file. The format is:

type <filename>

For example:

```
type config.da0
[CFG]
config last_saved "12:04:45, 31 Jan 2011"
config last_saved_changes "1"
config last_saved_user "ASY 0"
eth 0 descr "LAN 0"
eth 0 IPaddr "10.1.51.3"
eth 0 mask "255.255.0.0"
eth 0 bridge ON
eth 1 descr "LAN 1"
eth 2 descr "LAN 2"
eth 3 descr "LAN 3"
eth 4 descr "ATM PVC 0"
```

XMODEM File Transfer

The *xmodem* command is used to initiate an XMODEM file upload from the port at which the command is entered. The format is:

xmodem <filename>

where *<filename>* is the name under which the file will be saved when the upload is complete.

After entering the xmodem command the unit will wait for your terminal program to start transmitting the file. When the upload is complete and the file has been saved, the unit will respond with the OK result code.

A remote XMODEM upload can also be initiated by establishing a Telnet session over ISDN, and then issuing the xmodem command from the remote terminal.

USB Support

Most TransPort router come equipped with USB ports that you can use to connect Mass Storage Devices (MSDs) such as external hard drives or flash-memory pen drives. All the files on the USB device will be listed under the **USB Directory Listing** heading on the ***Administration - File Management > FLASH Directory*** page.

Note:
The USB storage device must be formatted using the FAT16 or FAT32 file system.

When the USB storage device is first inserted into the unit, the operating system looks for a file named “autoexec.bat”, and if found, executes it. Other batch files can be executed by pressing the reset button one or more times. The batch file to be executed must be called “pb<n>.bat”, where <n> is the number of times the reset button is to be pressed in order to execute the file.

SD Memory Card Support

Some TransPort routers are available with internal SD memory card, the drive letter assigned to this card is “s:”. To access the SD memory using an FTP client, the subdirectory assigned is “sdmmc”. The SD card can be used in the same way as USB MSDs. The SD card is internal and not removable.

Batch Control Commands

Any batch file can contain one of the following two control lines: ERROR_EXIT or ERROR_RUN. If ERROR_EXIT is specified in a batch file, any commands run after that point in the file will cause the termination of the batch file if that command causes an error (for example, attempting to delete a file that does not exist). ERROR_RUN can be used to return the operation to default, which is to continue the execution of the batch file commands.

USB Filing System Commands

The USB storage device will respond to any of the standard filing system commands. For all filing system commands, the USB storage device is regarded as drive u:.

Note:
The unit does not support sub-directories. Any sub-directories on the USB device will appear with a size of 0 bytes on the ***Administration - File Management > FLASH Directory*** page.

Example 1:

To display the contents of the USB storage device, you would enter the command:

```
dir u:
SERIALS.TXT 1843
EVENTL~1.TXT 1449
USB.TXT 4278
MASSR1~1.TXT 1255
OK
```

If the USB storage device is empty, you will get the following message:
```
No files
```

If no USB device is present, the following message is displayed:
```
No USB flash directory
```

Example 2:

To copy a file called “image” from the main flash memory onto the USB device, you would enter the command:

copy image u:image

To copy a file called “Logcodes.TXT” from the USB device to the main flash memory, you would enter the command:

copy u:Logcodes.TXT Logcodes.TXT

or

copy u:Logcodes.TXT

If no destination file is specified, the destination is set to the FLASH directory and the file name remains the same.

Using USB devices to upgrade firmware

Functionality available from firmware version 4891 onwards.

The firmware of a TransPort can be upgraded using the USB storage device. To do this procedure, using the information given above, a simple batch file called pb2.bat should created and the relevant files placed into the root directory of the USB storage device. Then, when the USB device is inserted into the TransPort and the reset button is pressed twice, the upgrade is performed.

```
ERROR_EXIT
del *.web
copy u:sbios1 sbios1
copy u:logcodes.txt logcodes.txt
copy u:image image
copy u:image4.c3 image4.c3
copy u:Y4890wVS.web Y4890wVS.web
move sbios1 sbios
scanr
flashleds
```

When the LEDs on the TransPort start flashing, the upgrade is complete and the TransPort must be rebooted for the new firmware to be activated.

Using USB devices with .all files

Functionality available from firmware version 4910 onwards.

A .all file is a special file that contains all of the firmware and configuration files in a single file that has the file extension .all and is an exact copy of the TransPort router in its current state. This .all file can then be applied to another TransPort router, as long as it is the same model.

To extract a .all file use the Digi Flash Writer software.

Copy the .all file to a USB storage device and insert the device into the TransPort router. Issue the command “dir u:” to confirm the TransPort can access the USB device. To copy the .all file onto the TransPort router, from the command line enter “copy u:mr4110.all t.all” (replacing mr4110.all with the correct .all file name and the t.all destination name can be anything). Please note that the source file (mr4110.all in this example) must adhere to the 8.3 filename convention (due to limits of the FAT file system) or the process will fail.

USB Security

In order to prevent unauthorised access to a TransPort unit using a USB storage device (e.g. inserting a USB storage device with an autoexec.bat file designed to copy usernames and passwords, etc.) the usbcon command can be used to define an access key. If the .bat file does not contain the matching key, it will not be allowed to execute. The put parameter of the uflash command is used to encode the key onto the file.

Note:
When using the uflash command, the filename should not be prefixed with u:, as the uflash command can only act on files stored on a USB storage device.

For example, to create a key you would enter the command:

usbcon 0 flashkey

In order to encode this key onto a file called “autoexec.bat” on the USB storage device, you would enter the command:

uflash autoexec.bat put

In order to remove a key from a file, you would use the clr parameter of the uflash command, thus:

uflash autoexec.bat clr

Note:
You must be logged onto the unit with **Super** access level in order to use the uflash command.

By default, an autoexec.bat file will be executed if found when a USB drive is inserted. Other batch files can also be executed. This behaviour can be controlled if required by issuing the command:

usbcon 0 batfile <off|on>

Disable/Enable the USB ports

If required, the external USB ports can be disabled to prevent any unauthorised copying of files to or from the router and prevent unauthorised use of flash drives or serial devices connected to the USB ports. This is also done with the usbcon command. The parameters used with the usbcon command are dislist to disable or enalist to explicitly enable a list of USB drivers. The driver list can be comma separated to specify more than one driver if required.

The format of the disable command is:

usbcon 0 usb-x-p<.p>.<DRIVER>

Where x=1 for the bottom USB port and 2 for the top port.

Where p=<port #> (if connected to a USB hub the port numbers can increase).

Where DRIVER = "MSD" for Mass Storage Device. "SERIAL" for serial devices, or "HUB" for hub devices.

To disable a Flash Stick on the top port only...

usbcon 0 dislist usb-2-2.MSD

Wildcards are also possible so to disable flash devices entirely. For example:

usbcon 0 dislist usb-.MSD*

This will match on ALL MSD devices even if in another HUB.

To disable both external USB ports on a DR64x0 the following commands can be used...

usbcon 0 dislist "usb-1-2,usb-2-2*"*

or

usbcon 0 dislist "usb-?-2"*

Note that the final -2 is important in both cases as otherwise the command would disable the internal USB devices which could include connections to the wireless module or other components.

To disable Serial devices from using either external USB port on a DR64x0, or on a port connected to a hub on either these ports...

usbcon 0 dislist "usb-1-2.SERIAL,usb-2-2*.SERIAL"*

or

usbcon 0 dislist usb-?-2.SERIAL*

The enalist takes the same format but when matches it causes the device to be specifically enabled. If a device matches the enable list as well as the disable list the enable list will take preference.

When a device matches a list an event is written to the event log of the form...

"USB device usb-1-2.4.MSD disabled"

or

"USB device usb-1-2.4.MSD enabled"

in the case the device matches the enalist.

These events can be used to debug the correct matching string to match on when trying to configure these parameters.

If both lists are left blank, all drivers are enabled and no extra events will appear in the event log.

Universal config.da0 using tags

The config.da0 contains a list of commands, one per line that are parsed at boot. The commands in this file differ depending on the model of the router, the firmware in use and the hardware options installed.

A single universal configuration file can be created with the use of tags, defining sections that only relate to a specific hardware type or firmware version.

The tag values that can be used are:

- The base model, for example: DR6410

- The complete model, for example: DR6410-H0A
- The platform build string, for example: 8W
- The type of DSL, for example: DSL2, 2+
- The type of WWAN module detected, for example: E (Edge), C (CDMA)
- The complete WWAN module string, for example: MOTO_G24, SIEMENS_GPRS, SIEMENS_MC75, NOVATEL_3G, SIERRA_3G, OPTION_3G, NOVATEL_CDMA, CMOTECH_CDMA, SIERRA_CDMA
  PSTN or ISDN module, for example: PSTN, ISDN

Tags must be used within angle brackets and the configuration sections must be opened AND closed with the relevant tag, for example: To open <DR6410>, to close </DR6410>. Note the use of the "/" in the closing tag.

To view a list of defined tags on a router, the CLI command tags can be used:

Example output of tags command:

```
Router>tags

tags defined:..

TransPort

DR64

dr6410

8W

OPTION_3G

ISDN

DSL

61690

OK
```

Example scenario:

A single configuration file is required for a range of DR6410 routers, there is a mix of 3 types of 3G WWAN modules and some have GPRS modules installed. Different W-WAN modules need different modemcc commands to correctly configure the ASY ports. All these modules can have their own specific commands in one config file.

Example configuration using tagged sections:

Comments are in red and prefixed with a # symbol. Comments may be used in configuration files to make them easier to read. The info_asy_add parameters are just for illustration purposes only and are not the actual ASY port numbers used.

```
<DR6410-H0A>
#Start of DR6410-H0A config

<NOVATEL_3G>
#Start of Novatel specific config
modemcc 0 asy_add 7
modemcc 0 info_asy_add 8
#End of Novatel specific config
</NOVATEL_3G>
```

```
<OPTION_3G>
#Start of Option specific config
modemcc 0 asy_add 7
modemcc 0 info_asy_add 9
#End of Option specific config
</OPTION_3G>

<SIERRA_3G>
#Start of Sierra specific config
modemcc 0 asy_add 7
modemcc 0 info_asy_add 10
#End of Sierra specific config
</SIERRA_3G>

#End of DR6410-H0A config
</DR6410-H0A>

<DR6410-E0A>
#Start of DR6410-E0A config
modemcc 0 asy_add 7
modemcc 0 info_asy_add 11
#End of DR6410-E0A config
</DR6410-E0A>

#Rest of generic config goes below here
modemcc 0 apn internet”
eth 0 ipaddr 192.168.0.99
```

Web GUI Access via Serial Connection

To access the web interface through one of the unit's serial ports (using Windows dial-up networking) follow the steps below.

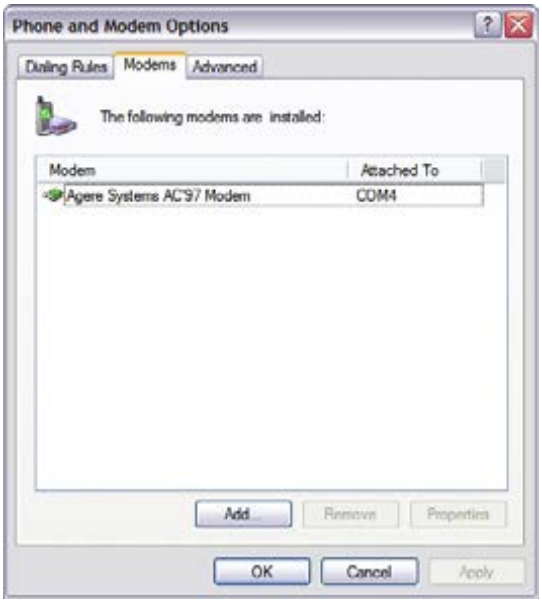
Note:
To use Dial-up Networking you must have the TCP/IP > Dial-up adapter installed in the Network Configuration for Windows. Check this by selecting Settings > Control Panel > Network > Configuration.

Installing the Driver File

You will need to install the "Digi_MULTI_PORT.INF" driver file and create a Windows PPP Dial-up Networking connection (DUN) for the unit as described below. It is assumed that you already have a basic knowledge of Windows networking concepts and terminology.

The precise procedure for installing the .inf driver file for the unit will vary slightly between different versions of Windows. The following description applies to Windows XP.

1. Start by selecting Start > Control Panel > Phone and Modem Options. You must be in Classic View. Select the Modems tab and you will see a dialog similar to the following:



2. Click on **Add...** to install a new modem driver:

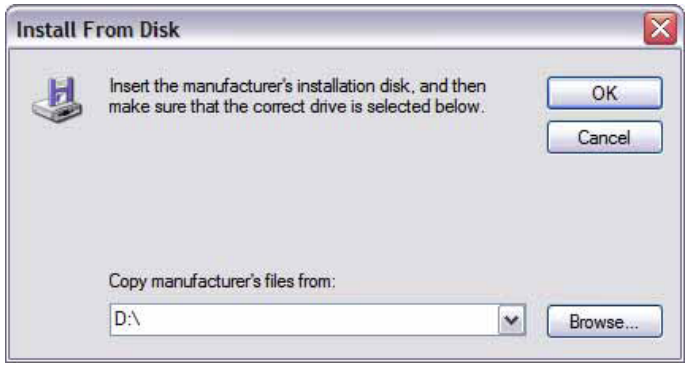

Add Hardware Wizard
Install New Modem
Do you want Windows to detect your modem?
Windows will now try to detect your modem. Before continuing, you should:
1. If the modem is attached to your computer, make sure it is turned on.
2. Quit any programs that may be using the modem.
Click Next when you are ready to continue.
Don't detect my modem; I will select it from a list.
< Back
Next >
Cancel

3. Check the Don't detect my modem, I will select it from a list option before clicking Next > to display the following dialog screen:


Add Hardware Wizard
Install New Modem
Select the manufacturer and model of your modem. If your modem is not listed, or if you have an installation disk, click Have Disk.
Manufacturer
(Standard Modem Types)
Models
Communications cable between two computers
Parallel cable between two computers
Standard 300 bps Modem
Standard 1200 bps Modem
This driver is digitally signed.
Tell me why driver signing is important
Have Disk...
< Back
Next >
Cancel

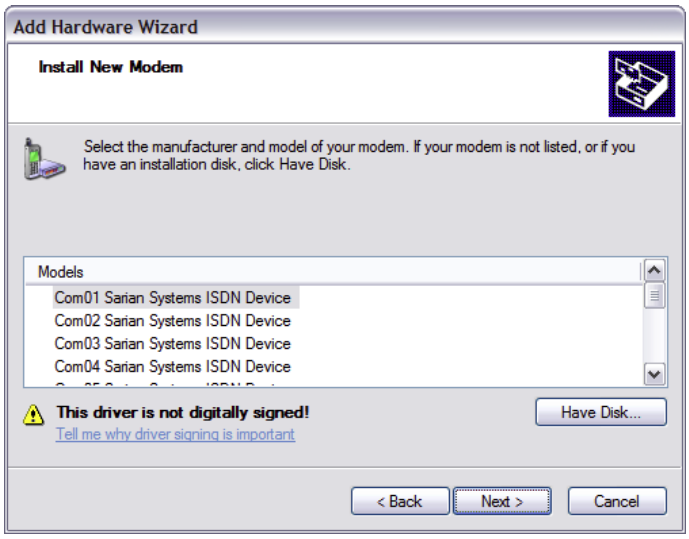
This screen lists the manufacturers and models of modem currently available on your system.

4. Insert the CD supplied into the CD drive and click on **Have Disk….**



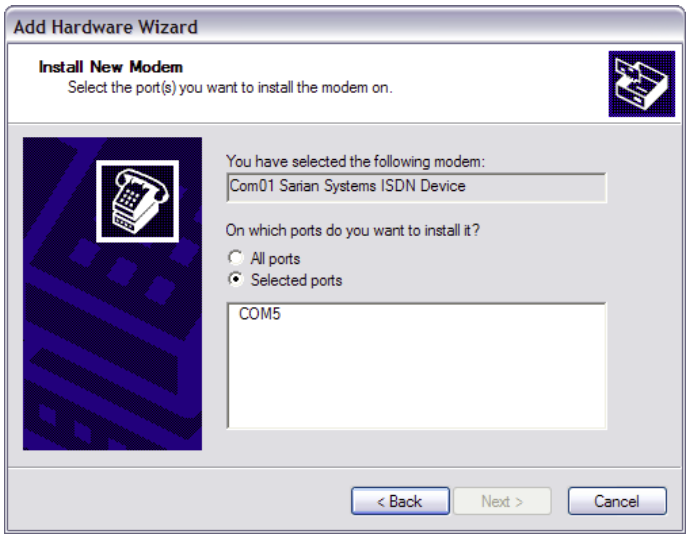
Use the **Browse** button to locate the Digi_MULTI_PORT.INF file on the driver CD supplied with your unit or downloaded from the Digi support website.

This will be in the appropriate Windows version sub-directory of the drives folder, e.g. win95-98. A list of routers will appear in the **Models** list:

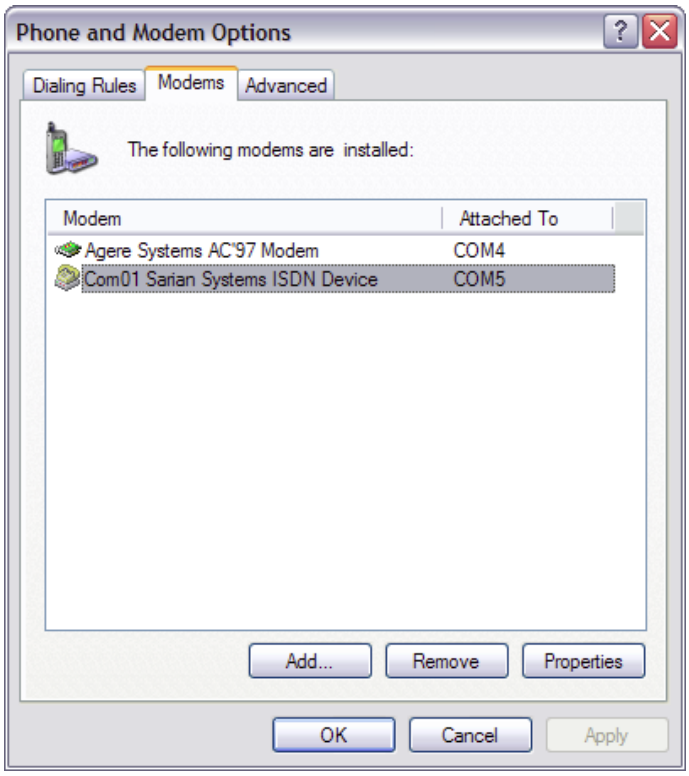

Add Hardware Wizard
Install New Modem
Select the manufacturer and model of your modem. If your modem is not listed, or if you have an installation disk, click Have Disk.
Models
Com01 Sarian Systems ISDN Device
Com02 Sarian Systems ISDN Device
Com03 Sarian Systems ISDN Device
Com04 Sarian Systems ISDN Device
This driver is not digitally signed!
Tell me why driver signing is important
Have Disk...
< Back
Next >
Cancel

Each entry in the list is the same driver, set up for a different COM port.

5. Choose the entry corresponding to the COM port your router is connected to, and click **Next >**. The wizard will ask you which COM port you wish to install the modem on.


Add Hardware Wizard
Install New Modem
Select the port(s) you want to install the modem on.
You have selected the following modem:
Com01 Sarian Systems ISDN Device
On which ports do you want to install it?
All ports
Selected ports
COM5
< Back
Next >
Cancel

6. Select the appropriate port and click **Next >**, and Windows will install the driver. Once installation is complete click **Finish** to return to the Phone and Modem Options dialog, where your unit will be listed:



Click on the **OK** button if you are satisfied with the installation.

Note:
During the installation you may receive a warning that the driver is not digitally signed. Click on Continue Installation to install the driver.

Creating A New Dial-Up Network Connection

You now need to create a new DUN connection through which you can access your unit.

If you are planning to connect the unit directly to your PC for configuration purposes, connect it to the appropriate COM port now using a suitable serial cable.

If you wish to configure a remote unit, make sure it is connected to a suitable ISDN line and make a note of the ISDN number.

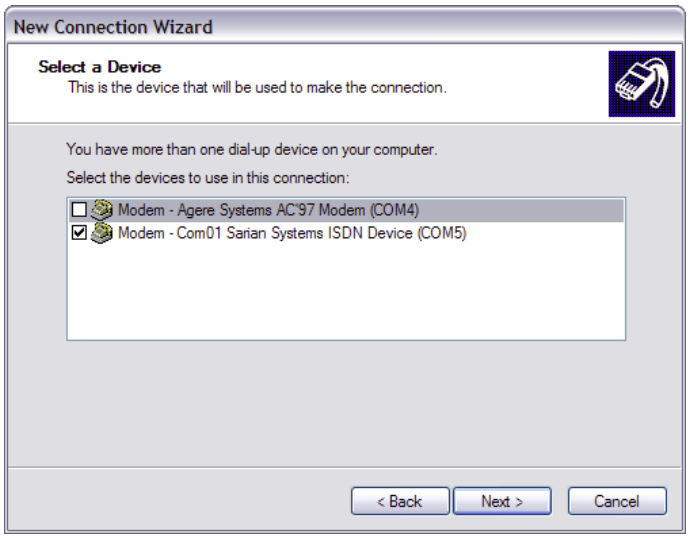
1. From the Windows Start menu, select All Programs > Accessories > Communications > New Connection Wizard. You will be presented with the New Connection Wizard introduction screen. Click on **Next >** to proceed to the Network Connection Type dialog:


New Connection Wizard
Network Connection Type
What do you want to do?
Connect to the Internet
Connect to the Internet so you can browse the Web and read email.
Connect to the network at my workplace
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.
Set up a home or small office network
Connect to an existing home or small office network or set up a new one.
Set up an advanced connection
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.
< Back
Next >
Cancel

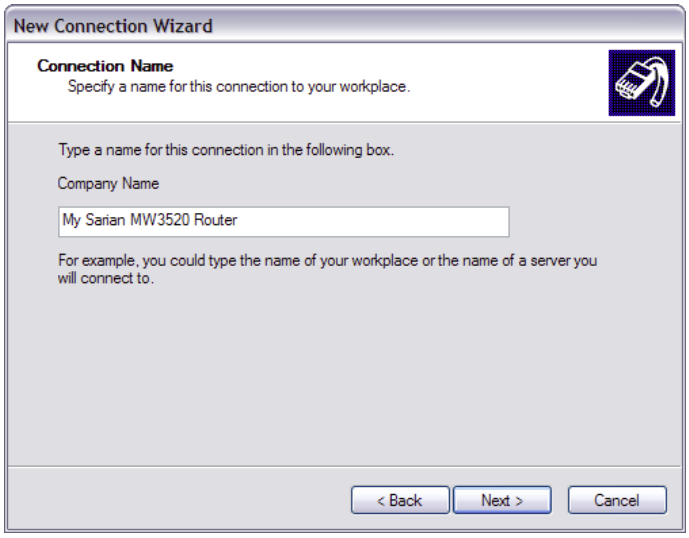
2. Select the **Connect to the network at my workplace** radio-button then click on **Next >**:


New Connection Wizard
Network Connection
How do you want to connect to the network at your workplace?
Create the following connection:
Dial-up connection
Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.
Virtual Private Network connection
Connect to the network using a virtual private network (VPN) connection over the Internet.
< Back
Next >
Cancel

3. Select the **Dial-up connection** radio-button then click on **Next >**:


New Connection Wizard
Select a Device
This is the device that will be used to make the connection.
You have more than one dial-up device on your computer.
Select the devices to use in this connection:
Modem - Agere Systems AC'97 Modem (COM4)
Modem - Com01 Sarian Systems ISDN Device (COM5)
< Back
Next >
Cancel

4. From the **Select a Device** dialog, select the unit you have just installed and make sure that any other devices in the list are unchecked. Click **Next >**.


New Connection Wizard
Connection Name
Specify a name for this connection to your workplace.
Type a name for this connection in the following box.
Company Name
My Sarian MW3520 Router
For example, you could type the name of your workplace or the name of a server you will connect to.
< Back
Next >
Cancel

5. You must now enter a name for the connection. It is helpful to choose a name that you will easily remember such as “My Digi Router” or “DR64 - Bristol Office”. Click **Next >**. The following dialog allows you to fill in the phone number for the connection:


New Connection Wizard
Phone Number to Dial
What is the phone number you will use to make this connection?
Type the phone number below.
Phone number:
123
You might need to include a "1" or the area code, or both. If you are not sure you need the extra numbers, dial the phone number on your telephone. If you hear a modem sound, the number dialed is correct.
< Back
Next >
Cancel

If the connection is being created for direct local access using a COM port, you should set the phone number to 123. This number will be intercepted by the unit and recognized as an attempt to connect locally.

If the connection is being created for remote access, enter the correct ISDN telephone number (including the area code) for the remote unit.

When you have done this click Next >. The final dialog screen will confirm that the connection has been created and includes a check box to allow you to create a shortcut on your desktop if necessary. Click on Finish to complete the task.

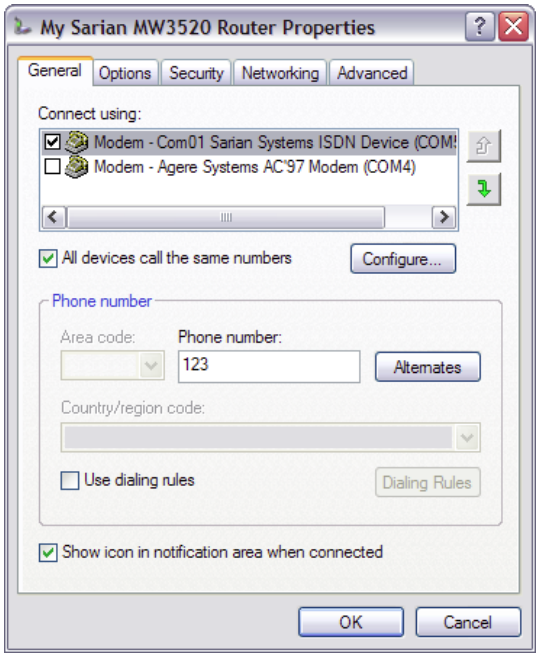
Configuring the New DUN Connection

The new DUN connection that you have just created may now be used to connect to the unit but before you do this, you will need to check some of the configuration properties.

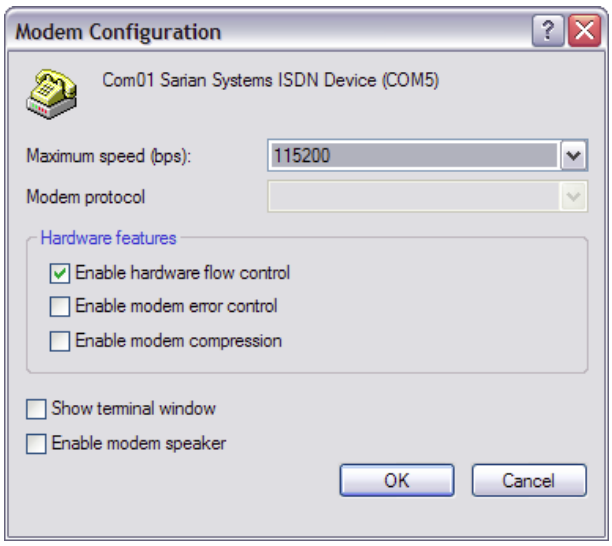
1. Click on the Start button and select Connect To > My Digi Router (substituting the connection name you chose).



2. Click on the **Properties** button to display the properties dialog for the connection:

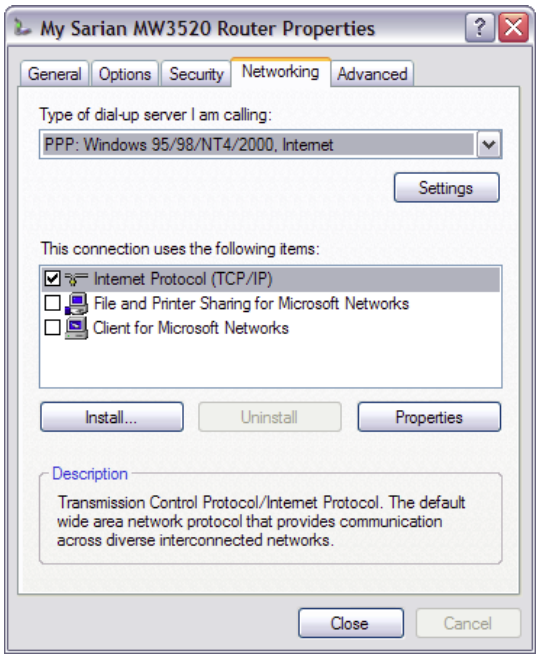


3. On the **General** tab, click the **Configure...** button to display the Modem Configuration dialog:

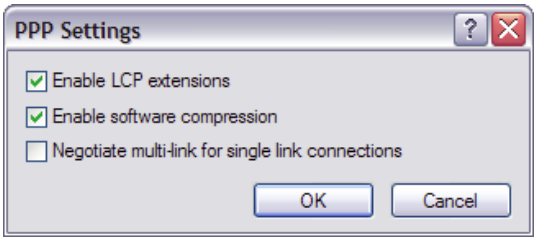


Make sure that the **Maximum speed (bps):** value is set to **115200** and that the **Enable hardware flow control** box is checked. Click **OK** when you have finished to return to the main properties dialog.

4. Now select the **Networking** tab:



Make sure that the Type of dial-up server I am calling is set to PPP: Windows 95/98/NT/2000, Internet and click on Settings:



Make sure that all three options are **unchecked** before clicking **OK** to return to the **Networking** tab. In the **This connection uses the following items** list, **Internet Protocol (TCP/IP)** should be the only item that is checked. Make sure that this is the case and then click **OK** to return to the main dialog. You are now ready to initiate a connection.

Initiating a DUN Connection

In the main dialog, you are asked to enter a username and password. The default settings for your unit are "**username**" and "**password**" respectively but you should change as soon as possible in order to prevent unauthorised access to your unit (refer to the section entitled Configuration - Security > Users for instructions on how to do this). The username is not case sensitive, but the password is.



Note:
When you type the password it will appear as a series of dots to ensure privacy.

Once you have entered these, initiate a connection to your unit by clicking the **Dial** button. During the dialling and connection process, you may see a series of status dialog boxes and, if the connection is successful, the final dialog box will indicate that the PPP login has been authenticated.

After a short delay, this dialog will minimise to a "linked computers" icon in the Windows taskbar:



You should now be ready to access the built-in web pages using your Web browser. The default "web address" for the unit is **http://1.2.3.4**. By default, this is also mapped to the system IP hostname **digi.router**.

You will need a valid username and password to access the web interface. Once again, the default settings are **username** and **password** respectively. If these values do not allow access, you should contact your system administrator.

SQL commands

When IPSec Egroups are used with a SQL database for dynamic Eroute configuration, there are CLI commands that will help with configuration and troubleshooting on the Digi router.

Local Database commands

As well as using an external SQL database, the Digi can cache the SQL table entries it learns from the SQL server in RAM so if the SQL server goes offline for any reason, the database entries are still available to renew existing IPSec SA's.

To configure the caching options the command used is *sql 0 <parameter> <value>*

The following parameters are available to configure the caching of database entries:

dbsrvmem <n>

This parameter is used to specify the amount of memory (RAM) the MySQL server cache should use. Where <n> is specified in multiples of 1k. e.g. 10Mb = 10240

To calculate the amount of memory to specify in this parameter:

1. Look at the size of the database file (.csv) that will be loaded into the Digi memory.

2. Double this value and add 100Kb, for example, if the csv file is 200Kb, this would make a value of 500Kb for the memory allocation. Use the command *sql 0 dbsrvmem 500*

3. Load the database file into memory and check the memory allocated and free using the *smem* command. This will show the memory allocated and left available. Increase the memory in the *dbsrvmem* command if required.

dbfile <name>

This is the name of the csv file that the Digi will use to store the table definitions (1st line) and data records. This file is stored in flash and is used to populate the database stored in RAM on power up or when a new file matching this name has just been stored. The dbfile can be populated with records or be empty except for the definitions line. The dbfile stored in RAM will be populated from both the dbfile stored in flash and (if configured) via caching items learnt from the main SQL server. The dbfile in flash can then be updated from the dbfile in RAM and saved.

dbname <name>

This is the name of the backup database in case the main database goes offline. This name needs to match the database name in use on the SQL server.

learn <off|on>

When enabled, the Digi will cache entries learnt via the main SQL database in a file stored in RAM. This can be used as a backup in the event of the main SQL database going offline. To use learning mode, at least one column in the csv dbfile must be marked as a unique key, with the U prefix.

For example, remip is marked as the unique key:

peerip[IP],bakpeerid[IP],peerid[K20],password[20],ourid[20],remip[UKIP],remmsk[IP]

Learning mode - Saving entries

When learning mode is used, the dynamic backup database is stored in RAM. This database will be lost if the Digi router is power cycled. The database in RAM can be saved to flash to over-write the dbfile with the one in RAM that includes the learnt entries or it can be saved to a new file.

To save the dbfile to flash from RAM, use the following command.

sqlsave 0 <filename>

Where *<filename>* is the name of the destination file.

For example, to save the learnt database entries to a file called backup.csv

sqlsave 0 backup.csv

If there are no learnt entries, this command will not create a file. To view the number to learnt entries, use the command sql 0 ? and refer to the section headed *Learning info*.

```
Learning info.
items learned:0
matched retrievals:0
OK
```

Configure a TransPort to use a backup database

Once the Digi has been configured to run a SQL csv database locally, this backup csv database can be used in the event of the main SQL database going offline. The configuration parameters required are:

Configure the IP address of the SQL server to use.

egroup 0 dbhost "192.168.0.50"

Configure the IP address of the SQL server that will have a backup database. If a socket connection fails to this IP address, the Digi will use the backup IP address.

ipbu 0 IPaddr "192.168.0.50"

Configure the backup database IP address. eg. the loopback address of the Digi router or an alternative SQL server, this eaxmple shows the loopback IP address of the Digi router.

ipbu 0 BUIPaddr "127.0.0.1"

Set the amount of time in seconds that the connection to the main SQL server will be retried.

ipbu 0 retrysec 30

Set the Digi to use the backup IP address if the main database is unavailable.

ipbu 0 donext ON

For example, to configure and use a local backup database when the main SQL database at 192.168.0.50 is offline, the configuration may look similar to this:

```
egroup 0 dbhost "192.168.0.50"
sql 0 dbsrvmem 200
sql 0 dbfile "sardb.csv"
sql 0 dbname "sarvpns"
sql 0 learn ON
sqlsave 0 backup.csv
ipbu 0 IPaddr "192.168.0.50"
ipbu 0 BUIPaddr "127.0.0.1"
ipbu 0 retrysec 30
ipbu 0 donext ON
```

Memory info

smem

Displays the amount of memory allocated, in use and available for use by the MySQL server on the Digi.

Transact SQL commands

To query a SQL database manually using transact SQL statements, the following commands can be used.

To connect to the SQL server and database:

sqlcon <host> <user> <pwd> <database>

For example:

sqlcon 192.168.0.50 sqluser sqlpass eroute-db

To issue transact SQL statements:

sqldo <"cmd">

For example:

*sqldo "select * from site where subnet='10.110.100.0' limit 3"*

To limit the sqldo command to only act on specified fields, the following command can be used:

sqlfields “<field1> <field2> <field3>”

For example:

sqlfields “remmsk password peerip”

After issuing the sqlfields command, all further sqldo commands will apply to these fields only.

When finished, to close the SQL server connection correctly:

sqlclose

If the database being queried is held locally on the Digi, these commands can be preceded with the SQL debug command to give extra feedback on any commands issued.

To enable the SQL debug:

sql 0 debug_opts 3

To view the debug data via the ASY 0 port:

debug 0

To view the debug data via telnet:

debug t

To disable the SQL debug:

sql 0 debug_opts 0

debug off

Answering V.120 Calls

V.120 is a protocol designed to provide high-speed point-to-point communication over ISDN. It provides rate adaptation and can optionally provide error control. Both the calling and called units must be configured to use V.120 before data can be transferred. Similarly, if one unit is configured to use the error control facility, the other must be configured in the same way.

Initial Set Up

Before using V.120 you must first bind one of the two available V.120 instances to the required ASY port using the ***Configuration - Network > Interfaces > Serial > Protocol Bindings*** page or by using the bind command from the command line, for example:

```
bind v120 0 asy 0
```

You should also select the appropriate method of flow control for the ASY port using the ***Configuration - Network > Interfaces > Serial > Serial Port n*** page or by using the AT&K command from the command line. Other ASY port options such as command echo, result code format, etc. should also be configured as necessary.

Initiating a V.120 Call

Once the initial configuration is complete, V.120 calls may be initiated using the appropriate ATD command. For example:

```
atd01234567890
```

A successful connection will be indicated by a CONNECT result code being issued to the ASY port and the unit will switch into on-line mode. In this mode, all data from the terminal attached to the bound ASY port will be passed transparently through the unit across the ISDN network to the remote system. Similarly, all data from the remote system will be passed directly to the terminal attached to the bound ASY port.

If a V.120 call fails the unit will issue the NO ANSWER or NO CARRIER result code to the ASY port and remain in command mode.

The ATD command may also be used to route a call to an ISDN sub-address by following the telephone number with the letter S and the required sub-address value. For example:

```
atd01234567890s003
```

In this case, the remote system will only answer the call if it has been configured to accept incoming calls on the specified sub-address.

Answering V.120 Calls

V.120 answering can be enabled from the command interface by setting register S0 for the appropriate ASY port to a non-zero value. For example:

```
ats0=1
```

You should ensure that you have set S0 for the correct ASY port by either entering it directly on that port or by using the AT\PORT command to select the correct port first.

The actual value used for the parameter sets the number of rings the unit will wait before answering.

Finally, you must ensure that there are no conflicts with other protocols configured to answer on other ASY ports. This can be done by disabling answering for the other ports/protocols or by using the MSN and/or Sub-address parameters to selectively answer calls to different telephone numbers using different protocols.

For example, if you have subscribed to the ISDN MSN facility, you may have been allocated say four telephone numbers ending in 4, 5, 6 and 7. You could then set the MSN parameter for the appropriate V.120 instance to 4 to configure V.120 to answer only incoming calls to the MSN number ending in 4.

You should check that if PPP answering is enabled you have NOT selected the same MSN and Sub-address values for PPP. If they are the same, V.120 will answer the call ONLY if S0 is set to 1. Otherwise, PPP will take priority and answer the call.

ANSWERING ISDN CALLS

Digi routers are capable of answering incoming B-channel ISDN calls with 3 main protocols. Usually several instances of these protocols exist. This section explains how answering priorities work for the different protocols.

Protocol Entities

The following protocol instances are capable of answering an incoming ISDN call:

Adapt

Adapt instances provide rate adaptation protocols such as V.120 or V.110.

LAPB

LAPB instances allow the unit to answer incoming X.25 calls over ISDN. They can optionally connect the caller to a synchronous serial port, an asynchronous serial port bound to a PAD, or switch the call to another interface.

PPP

IP data tunnelled over PPP instances allow remote access to the unit's IP-based management features and also facilitate onward IP routing through any of the unit's IP enabled interfaces.

The unit will automatically answer an incoming ISDN call if any of the following statements are true (subject to the entity MSN, Calling Number and Sub-address parameters being set to their default values):

- An Adapt instance is bound to an asynchronous serial port (ASY) and the answer ring count (S0) for that serial port is set to 1
- A LAPB instance has its answering parameter set to On
- A PPP instance has its answering parameter set to On

If more than one of these protocols are configured to auto answer then the priority is as follows:

Adapt instances (normally V.120) will take priority over LAPB, which will take priority over PPP. If an Adapt instance is bound to an asynchronous serial port (ASY port) but the answer ring count (ATS0) is not set to 1 for that same serial port then Adapt entity will not answer automatically. If any other protocol entities (e.g. LAPB, PPP or another Adapt instance) are configured to answer then one of these protocol entities will answer the call. If no other protocol entities are configured to answer then a repeating RING message will be sent out of the serial port and the RS232 ring indicator control will be activated. If a terminal attached to the serial port sends ATA followed by carriage return then the ISDN call will be answered by the Adapt entity and any incoming data will be channelled out of the serial port and vice-versa.

Multiple Subscriber Numbers

An MSN (multiple subscriber number) is an alternative number provided by the telephone service provider which when dialled will also route through to your ISDN line. It is possible to purchase several MSNs for an ISDN line. This means that in effect one ISDN line can have several ISDN numbers.

Every entity in the router which is capable of answering an ISDN call (Adapt, LABP and PPP) has an MSN parameter.

A protocol entity's MSN parameter can be used to:

• cause a protocol instance not to answer an incoming ISDN call (if the trailing digits of the ISDN number called do not match the entry in this field).

• increase the answering priority of an instance (if more than one protocol instance is configured to answer and the trailing digits of the ISDN number called match the value of the MSN parameter for a particular protocol instance).

Example

Consider the following:

- an Adapt instance is bound to a serial port and ATS0 for that serial port is set to 1
- PPP instance 0 has answering turned On
- the ISDN line to which the router is connected has two numbers: the main number is 123456 and the MSN number is 123789

Normally, because ADAPT has a higher answering priority than PPP, the Adapt instance will answer when either of the numbers are called. However if the ISDN number dialled is 123456 and 456 is entered into the MSN parameter of PPP then PPP will answer instead. This will also have the effect of preventing PPP from answering if any other ISDN number (e.g. 123457) has been called.

This means that whenever 123456 is called the PPP instance will answer and that whenever 123789 is called the V120 instance will answer.

It is possible to connect multiple ISDN devices to the same ISDN line. MSNs can then be used to allow the different ISDN devices to be dialled individually (i.e. dial the main ISDN number and get through to ISDN device one, dial the first MSN and get through to ISDN device number two, dial the second MSN and get through to ISDN device number three, etc.).

Multiple PPP Instances

It is also possible to configure multiple instances of a particular entity to answer. For example, PPP instance, 0, 1 and 4 could be configured to answer. In this case provided that none of the PPP instances are busy, the PPP instance with the highest number will answer first. MSNs can also be used to ensure that a chosen PPP instance answers the call.

Multiple protocol entity answering instance rules:

ADAPT

The lowest free Adapt instance with auto-answering enabled will answer first.

PPP

The lowest free PPP instance with answering on will answer first.

LAPB

The lowest free LAPB instance with answering on will answer first.

X.25 PACKET SWITCHING

Introduction

X.25 is a data communications protocol that is used throughout the world for wide area networking across Packet Switched Data Networks (PSDNs). The X.25 standard defines the way in which terminal equipment establishes, maintains and clears Switched Virtual Circuits (SVCs), across X.25 networks to other devices operating in packet mode on these networks.

The protocols used in X.25 operate at the lower three layers of the ISO model. At the lowest level the Physical layer defines the electrical and physical interfaces between the DTE and DCE. Layer 2 is the Data Link Layer that defines the unit of data transfer as a “frame” and includes the error control and flow control mechanisms. Layer 3 is the Network layer. This defines the data and control packet structure and the procedures used to access services that are available on PSDNs.

A further standard, X.31 defines the procedures used to access X.25 networks via the ISDN B and D-channels.

Digi ISDN products include support for allowing connected terminals to access X.25 over ISDN B channels, the ISDN D-channel or over TCP. They can also be configured so that if there is a network failure it will automatically switch to using an alternative service. The Packet Assembler/Disassembler (PAD) interface conforms to the X.3, X.28 and X.29 standards.

Up to six PAD instances (from an available pool of 8), can be created and dynamically assigned to the asynchronous serial ports or the REM pseudo-port.

Each application that uses the unit to access an X.25 network will have its own particular configuration requirements. For example, you may need to program your Network User Address (NUA) and specify which Logical Channel Numbers (LCNs) should be used on your X.25 service. This information will be available from your X.25 service provider. You will also need to decide whether your application will use B or D-channel X.25.

Once you have this information, the PAD configuration pages can be used to set up the appropriate parameters.

B-channel X.25

The unit can transfer data to/from X.25 networks over either of the ISDN B-channels.

Once the unit has been configured appropriately, the ISDN call to the X.25 network can be made using an ATD command or by executing a pre-defined macro. The format of the ATD command allows you to combine the ISDN call and the subsequent X.25 call in a single command. Alternatively, the X.25 call may be made separately from the PAD> prompt once the ISDN connection to the X.25 network has been established.

D-channel X.25

The unit can transfer data to/from X.25 networks over the ISDN D-channel if your ISDN service provider supports this facility. The speed at which data can be transferred varies depending on the service provider but is generally 9600bps or less.

X.28 Commands

Once an X.25 session layer has been established the unit switches to “PAD” mode. In this mode operation of the PAD is controlled using the standard X.28 PAD commands listed in the following table:

Command	Description
CALL	Make an X.25 call
CLR	Clear an X.25 call
ICLR	Invitation to CLR
INPAR?	List X.3 parameters of specified PAD instance
INPROF	Load or save specified PAD profile
INSET	Set X.3 parameters of specified PAD instance
INT	Send Interrupt packet
LOG	Logoff and disconnect
PAR?	List local X.3 parameters
PROF	Load or save PAD profile
RESET	Send reset packet
RPAR?	List remote X.3 parameters
RSET	Set remote X.3 parameters
SET	Set local X.3 parameters
STAT	Display channel status

CALL Make an X.25 Call

The full structure of a CALL command is:

CALL [<facilities->]<address>[D<user data>]

where:

<facilities-> is an optional list of codes indicating the facilities to be requested in the call (separated by commas, terminated with a dash)

<address> is the destination network address.

<user data> is any optional user data to be included with the call.

The facility codes supported are:

F	Fast select - no restriction
Q	Fast select - restricted response
Gnn	Closed User Group
Gnnnn	Extended Closed User Group
R	Reverse charging
N<NUI>	Network User Identity code (NUI)

Example

CALL R,G12,NMYNUI-56512120DHello

places a call to address 56512120 using reverse charging and specifying Closed User Group 12. The string “MYNUI” is your Network User Identity and the string “Hello” appears in the user data field of the call packet.

Note:
The particular facilities that are available will vary between X.25 service providers.

If a CALL command is issued without the address parameter, it is assumed that you wish to go back on-line to a previously established call (having used the PAD recall facility to temporarily return to the PAD> prompt).

Fast select (ISDN B-channel only)

When the standard Fast select facility is requested using the “F” facility code, the call packet generated by the CALL command is extended to allow the inclusion of up to 124 bytes of user data. For example:

CALL F-1234567890DThis DATA sent with call packet

would cause an X.25 CALL packet to be sent using the Fast select facility including the message “This DATA sent with call packet” (the Carriage Return used to enter the command is not transmitted). Without the inclusion of the Fast select facility code, only the first 12 characters would be sent.

When a Fast select CALL has been made the PAD accepts an extended format response from the called address. This response, consisting of up to 124 bytes of user data, may be appended to the returning call accepted or call clear packet. When one of these packets is received, the user data is extracted and passed from the PAD to the terminal immediately prior to the “CLR DTE . . .” message in the case of a call clear packet or “CON COM” message in case of a call accepted packet.

When a restricted response Fast select call has been made using the Q facility code, the call packet indicates that a full connection is not required so that any response to the user data in the CALL packet should be returned in a call clear packet.

When the PAD receives an incoming call specifying Fast select, the call is indicated to the terminal in the normal way. For example:

IC 1234567890 FAC: Q,W:2 COM

would indicate that an incoming call had been received requesting Restricted response fast select and a window size of 2. The user (or system) then has 15 seconds in which to pass up to 124 bytes of data to the PAD to be included in the clear indication packet that is sent in response to the call.

The PAD does NOT differentiate between standard and restricted response Fast select on incoming calls and, consequently, will always respond with a clear indication.

Network User Identity (NUI)

The N facility code allows you to include your Network User Identity in the call packet. For security reasons the PAD echoes each character as an asterisk (*) during the entry of an NUI. Some X.25 services use the NUI field to pass both a username and password for validation. For example, if your Username is MACDONALD and your password is ASDF, a typical CALL command would have the format:

CALL NMACDONA;ASDF-56512120

where the ";" is used to separate the username from the password.

Closed User Group (CUG)

Most X.25 networks support Closed User Groups. They are used to restrict subscribers to only making calls or receiving calls from other members of the same CUG. The CUG number effectively provides a form of sub-addressing that is used in conjunction with the NUA to identify the destination address for a call.

When the G facility code is specified in a CALL packet, it must be followed by the CUG number. This may be a 2 or 4 digit number. If you are a member of a closed user group, the network may restrict you to only making calls to or receiving calls from other members of the same group.

Reverse charging

Reverse charging, specified using the R facility code, allows outgoing calls to be charged to the account of destination address. Whether or not a call is accepted on a reverse charging basis is determined by the service provider and by the type of account held by the called user.

Calling user data

The calling user data field for a normal call may contain up to 12 bytes of user data. If the first character is an exclamation mark (!), the PAD omits the four byte protocol identifier and allows the full 16 bytes as user data. The same is true for a fast select call except that the maximum amount of user data is increased from 124 to 128 bytes.

When entering user data, the tilde character (~) may be used to toggle between ASCII and binary mode. In ASCII mode data is accepted as typed but in binary mode each byte must be entered as the required decimal ASCII code separated by commas. For example to enter the data "Line1" followed by [CR][LF] and "Line2" you would enter:

DLine1~13,10~Line2

Aborting a CALL

An X.25 CALL may be aborted using the X.28 CLR command, by pressing [Enter] or by dropping DTR from the terminal while the call is in progress. Dropping DTR will also terminate an established call.

If a call is terminated by the network or by the remote host, the unit returns a diagnostic message before the NO CARRIER result code. Messages may be numeric or verbose depending on the setting of the ATV command.

The following table lists the verbose messages and equivalent numeric codes:

Code	Verbose message
1	Unallocated (unassigned) number
2	No route to specified transit network

Code	Verbose message
3	No route to destination
4	Channel unacceptable
6	Channel unacceptable
7	Call awarded and being delivered in an established channel
16	Normal call clearing
17	User busy
18	No user responding
19	No answer from user (user alerted)
21	Call rejected
22	Number changed
26	Non-selected user clearing
27	Destination out of order
28	Invalid number format
29	Facility rejected
30	Response to STATUS ENQUIRY
31	Normal, unspecified
34	No circuit/channel available
38	Network out of order
41	Temporary failure
42	Switching equipment congestion
43	Access information discarded
44	Requested circuit/channel not available
47	Resources unavailable, unspecified
49	Quality of service unavailable
50	Requested facility not subscribed
57	Bearer capability not authorized
58	Bearer capability not presently available
63	Service or option not available, unspecified
65	Bearer capability not implemented
66	Channel type not implemented
69	Requested facility not implemented
70	Only restricted digital information bearer
79	Service or option not implemented, unspecified
81	Invalid call reference value

Code	Verbose message
82	Identified channel does not exist
83	A suspended call exists, but this call identity does not
84	Call identity in use
85	No call suspended
86	Call having the requested call identity has been cleared
88	Incompatible destination
90	Destination address missing or incomplete
91	Invalid transit network selection
95	Invalid message, unspecified
96	Mandatory information element is missing
97	Message type non-existent or not implemented
98	Message not compatible with call state or message type nonexistent or not implemented
99	Information element non-existent or not implemented
100	Invalid information element contents
101	Message not compatible with call state
102	Recovery on timer expired
111	Protocol error, unspecified
127	Interworking, unspecified
128	General level 2 call control failure (probable network failure)

Note:
Some verbose messages may be abbreviated by the unit.

CLR Clear an X.25 Call

The CLR command is used to clear the current call and release the associated virtual channel for further calls. On completion of call clear the PAD> prompt is re-displayed. A call may also be cleared as a result of a number of other situations. If one of these situations occurs, a message is issued to the PAD in the following format:

CLR <Reason> C:<n> - <text>

where:

<*Reason*> is a 2/3 character clear down code

<*n*> is the numeric equivalent of the clear down code

<*text*> is a description of the reason for clear down

The clear down reason codes supported by the unit are listed in the following table:

Reason Code	Numeric Code	Text
DTE	0	by remote device
OOC	1	number busy
INV	3	invalid facility requested
NC	5	temporary network problem
DER	9	number out of order
NA	11	access to this number is barred
NP	13	number not assigned
RPE	17	remote procedure error
ERR	19	local procedure error
ROO	21	cannot be routed as requested
RNA	25	reverse charging not allowed
ID	33	incompatible destination
FNA	41	fast select not allowed
SA	57	ship cannot be contacted

If an unknown reason code is received, the text field is blank.

ICLR Invitation To CLR

The ICLR command “invites” the remote X.25 service to CLR the current X.25 session.

INT Send Interrupt Packet

INT causes PAD to transmit an interrupt packet. These packets flow “outside” normal buffering/flow control constraints and are used to interrupt the current activity.

LOG Logoff and Disconnect

LOG is used to terminate an X.25 session. It causes the PAD to clear any active X.25 calls, disconnect and return to AT command mode.

PAR? List Local X.3 Parameters

PAR? lists the local X.3 parameters for the current session.

PROF Load/Save PAD Profile

The PROF command is used to store or retrieve a pre-defined set of X.3 PAD parameters (referred to as a PAD profile). The information is stored in system file called X3PROF. There are four pre-defined profiles numbered 50, 51, 90 and 91. Additionally, you may create four “user PAD profiles” numbered 1 to 4.

Profile 50 is automatically loaded when a PAD is first activated. To load one of the other pre-defined profiles use the PROF command followed by the required profile number. For example:

PROF 90

To create a User PAD profile you must use the SET command to configure the various PAD parameters to suit your application and then use the PROF command in the format:

PROF &nn

where “nn” is the number of the User PAD profile to be stored, e.g. 03. Alternatively, you may use the web interface to edit the parameters directly (***Configuration - Network > Legacy Protocols > X.25 > PADs n-n > PAD n > PAD Settings***).

The pre-defined profiles (50, 51, 90, 91), cannot be overwritten and are permanently configured as shown in the following table:

Parameter	Profile			
	50	51	90	91
1	1	0	1	0
2	0	0	1	0
3	0	0	126	0
4	5	5	0	20
5	0	3	1	0
6	5	5	1	0
7	0	8	2	2
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	15	15	15	15
12	0	3	1	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	8	8	127	127
17	24	24	24	24
18	18	18	18	18
19	2	2	1	1
20	64	64	0	0
21	0	0	0	0
22	0	0	0	0

Stored X.25 PAD profiles are held in non-volatile memory and will not be lost when the unit is switched off.

When used in the format:

prof nn

the PROF command loads the stored profile specified by “nn”.

RESET Send Reset Packet

RESET is used to issue a reset for the current call to the network. It does NOT clear the call but it does return the network level interface to a known state by re-initialising all Level 3 network control variables. All data in transit will be lost.

RPAR? Read Remote X.3 Parameters

RPAR? lists the current X.3 parameter settings for the remote system.

RSET Set Remote X.3 Parameters

RSET is used to set one or more X.3 parameters for the remote system. It is entered in the format:

RSET par #:value[,par #:value[,par #:value ...]]

SET Set Local X.3 Parameters

SET is used to set one or more of the local X.3 parameters for the duration of the current session. The format of the command is:

SET par #:value[,par #:value[,par #:value ...]]

STAT Display Channel Status

STAT displays the current status for each logical channel indicating whether it is free or engaged. For example:

```
stat
PAD   STATE
1     ENGAGED
2     FREE
3     FREE
4     FREE
```

PPP OVER ETHERNET

PPP over Ethernet (PPPoE) is a means of establishing a PPP connection over the top of an Ethernet connection. The implementation provided is compliant with RFC 2516, “A Method for Transmitting PPP Over Ethernet”. A typical application would be to allow non-PPPoE enabled devices to access Internet services where the connection to the Internet is provided by an ADSL bridge device.

Using the Web Page(s)

There is no dedicated web page for configuring the unit to use PPPoE; rather there are a number of parameters that appear on other web pages that must be used in conjunction with each other to establish a PPPoE connection over the appropriate Ethernet interface.

In particular, the following configuration pages and parameters are important.

On the appropriate ***Configuration - Network > Interfaces > Advanced > PPP n - n*** pages, you should configure the following parameters on the following pages:

Configuration - Network > Interfaces > Advanced > PPP n - n > PPP n

As a minimum requirement the **Username** and **Password** parameters should be initialised.

The parameter **This PPP interface will use x,y** defines the physical Ethernet interface over which the PPPoE session will operate. In most cases this is PPPoE 0 (for Ethernet 0). The fact that you have selected “PPPoE 0” as the physical interface for operation with PPP automatically enables PPPoE mode. If another Ethernet instance is used, Eth 1 for example, this will need to be specified as PPPoE 1 to ensure the correct MAC address is used, this is in the format 0 or blank for port 0, 1 for port 1, 2 for port 2 etc.

If necessary, continue to the page ***Configuration - Network > Interfaces > Advanced > PPP n - n > PPP n > Advanced*** and set the **Enable "Always On" mode of this interface** parameter to “**On**” to configure the unit so that it will attempt to renegotiate the PPP link should it go down for any reason.

Configuration - Network > Interfaces > Advanced > PPP n - n > PPP n > PPP Negotiation

The **advanced PPP options** on this page should be initialised as required by your ISP.

In addition:

Desired Local MRU and **Desired Remote MRU** should be set to “1492”.

Request Local ACFC and **Request Remote ACFC** should be set to “No”.

Request Local PFC and **Request Remote PFC** should be set to “No”.

Desired Local ACCM and **Desired Remote ACCM** should be set to “0xffffffff”.

Using Text Commands

There are no specific PPPoE commands available to the user via the text command interface. The appropriate *ppp* CLI commands should be used to set the required options.

IPSEC AND VPNS

What is IPSec?

One inherent problem with the TCP protocol used to carry data over the vast majority of LANs and the Internet is that it provides virtually no security features. This lack of security, and recent publicity about “hackers” and “viruses”, prevent many people from even considering using the Internet for any sensitive business application. IPSec provides a remedy for these weaknesses adding a comprehensive security “layer” to protect data carried over IP links.

IPSec (Internet Protocol Security) is a framework for a series of IETF standards designed to authenticate users and data, and to secure data by encrypting it during transit. The protocols defined within IPSec include:

- IKE – Internet Key Exchange protocol
- ISAKMP – Internet Security Association and Key Management Protocol
- AH – Authentication Header protocol
- ESP – Encapsulating Security Payload protocol
- HMAC – Hash Message Authentication Code
- MD5 – Message Digest 5
- SHA-1 – Security Hash Algorithm

and the cryptographic (encryption) techniques include:

- DES – Data Encryption Standard
- 3DES – Triple DES
- AES – Advanced Encryption Standard (also known as Rijndael)

Two key protocols within the framework are AH and ESP. AH is used to authenticate users, and ESP applies cryptographic protection. The combination of these techniques is designed to ensure the integrity and confidentiality of the data transmission. Put simply, IPSec is about ensuring that:

- only authorised users can access a service and
- that no one else can see what data passes between one point and another.

There are two modes of operation for IPSec, transport mode and tunnel mode.

In transport mode, only the payload (i.e. the data content), of the message is encrypted. In tunnel mode, the payload and the header and routing information are all encrypted thereby by providing a higher degree of protection.

Data Encryption Methods

There are several different algorithms available for use in securing data whilst in transit over IP links. Each encryption technique has its own strengths and weaknesses and this is really, a personal selection made with regard to the sensitivity of the data you are trying to protect. Some general statements may be made about the relative merits but users should satisfy themselves as to suitability for any particular purpose.

DES (64-bit key)

This well-known and established protocol has historically been used extensively in the banking and financial world. It is relatively “processor intensive”, i.e. to run efficiently at high data rates a powerful processor is required. It is generally considered very difficult for casual hackers to attack but may be susceptible to determined attack by well-equipped and knowledgeable parties.

3-DES (192-bit key)

Again, this is a well-established and accepted protocol but as it involves encrypting the data three times using DES with a different key each time, it has a very high processor overhead. This also renders it almost impossible for casual hackers to attack and very difficult to break in any meaningful time frame, even for well-equipped and knowledgeable parties.

AES (128-bit key)

Also known as Rijndael encryption, AES is the new “de-facto” standard adopted by many USA and European organisations for sensitive applications. It has a relatively low processor overhead compared to DES and it is therefore possible to encrypt at higher data rates. As with 3-DES, it is almost impossible for casual hackers to attack and is very difficult to break in any meaningful time frame, even for well-equipped and knowledgeable parties.

To put these into perspective, common encryption programs that are considered “secure” (such as PGP) and on-line credit authorisation services (such as Web-based credit card ordering) generally use 128-bit encryption.

Note:
Data rates are the maximum that could be achieved but may be lower if other applications are running at the same time or small IP packet sizes are used.

What is a VPN?

VPNs (Virtual Private Networks) are networks that use the IPSec protocols to provide one or more secure routes or “tunnels” between endpoints. Users are issued either a shared “secret” key or “public/ private” key pair that is associated with their identity. When a message is sent from one user to another, it is automatically “signed” with the user’s key. The receiver uses the secret key or the sender’s public key to decrypt the message. These keys are used during IKE exchanges along with other information to create session keys that only apply for the lifetime of that IKE exchange.

The Benefits of IPSec

IPSec is typically used to attain confidentiality, integrity, and authentication in the transport of data across inherently insecure channels. When properly configured, it provides a highly secure virtual channel across cheap, globally available networks such as the Internet, or creates a “network within a network” for applications such as passing confidential information between two users across a private network.

X.509 Certificates

In the previous section, security between two points was achieved by using a "pre-shared secret" or password. Certificates provide this sort of mechanism but without the need to manually enter or distribute secret keys. This is a complex area but put simply a user's certificate acts a little like a passport providing proof that the user is who they say they are and enclosing details of how to use that certificate to decrypt data encoded with it. Passports however can be forged so there also needs to be proof that the passport has been properly issued and hasn't been changed since it was. On a paper passport this is achieved by covering the photograph with a coating that shows if it has been tampered with, embedding the user's name in code in a long string of numbers, etc. In the same way, for a Security Certificate to be genuine it has to be protected from alteration as well. Like a passport, you also have to trust that the issuer is authorized and competent to create the certificate.

Certificates use something called a "Public/Private Key Pair". This a complex area but the principle is that you can create an encryption key made up from two parts, one private (known only to the user), the other public (known to everyone). Messages encrypted with someone's public key can only be recovered by the person with the Public AND Private key but as encrypting the message to someone in the first place only requires that you know their public key, anyone who knows that can send them an encrypted message, so you can send a secure message to someone knowing only their publicly available key. You can also prove who you are by including in the message your "identity" whereupon they can look up the certified public key for that identity and send a message back that only you can understand. The important principles are that a) your private key cannot be determined from your public key and b) you both need to be able to look up the others certified ID. Once you've established a two way secure link you can use it to establish some rules for further communication.

Before this gets any more complicated we'll assume that Digi International are a competent authority to issue certificates and given that they exist and are valid, see how they are used.

Generally, the issuing and management of certificates will be provided as a managed service by Digi or its partners, but some general information is provided here for system administrators.

Certificates are held in non-volatile files on the unit. Any private files are named privxxxx.xxx and cannot be copied, moved, renamed, uploaded or typed. This is to protect the contents. They can be overwritten by another file, or deleted.

Two file formats for certificates are supported:

- PEM – Privacy Enhanced MIME
- DER – Distinguished Encoding Rules

Certificate and key files should be in one of these two formats, and should have an extension of ".pem" or ".der" respectively.

Note:
The equivalent filename extension for .PEM files in Microsoft Windows is ".CER". By renaming ".PEM" certificate files to ".CER", it is possible to view their makeup under Windows.

The unit maintains two lists of certificate files. The first is a list of “Certificate Authorities” or CAs. Files in this list are used to validate public certificates sent by remote users. Public certificates must be signed by one of the certificates in the CA list before the unit can validate them. Certificates with the filename CA*.PEM and CA*.DER are loaded into this list at start-up time. In the absence of any CA certificates, a public certificate cannot be validated.

The second list is a list of public certificates that the unit can use to obtain public keys for decrypting signatures sent during IKE exchanges. Certificates with a filename CERT*.PEM and CERT*.DER are loaded into this list when the unit is powered on or rebooted. Certificates in this list will be used in cases where the remote unit does not send a certificate during IKE exchanges. If the list does not contain a valid certificate communication with the remote unit cannot take place.

Both the host and remote units must have a copy of a file called CASAR.PEM. This file is required to validate the certificates of the remote units.

In addition, the host unit should have copies of the files CERT02.PEM (which allows it to send this certificate to remote units) and PRIVRSA.PEM. Note that before it can send this certificate, the “Remote ID” parameter in the Configuration - Network > Virtual Private Networking (VPN) > IPsec > IPsec Tunnels > IPsec n - n > IPsec n page must be set to “host@Digi.co.uk”.

The remote unit must have copies of CERT01.PEM and PRIVRSA.PEM. In addition, any Eroutes that are going to use certificates for authentication should be configured as follows:

Our ID

Should be set to “info@Digi.co.uk”. This is the same as the subject “Altname” in certificate CERT01.PEM which makes it possible for the router to locate the correct certificate to send to the host.

Authentication Method

Should be set to RSA Signatures. This indicates to IKE that RSA signatures (certificates) are to be used for authentication.

When IKE receives a signature from a remote unit, it needs to be able to retrieve the correct public key so that it can decrypt the signature, and confirm that the signature is correct. The certificate must either be on the FLASH file system, or be provided by the remote unit as part of the IKE negotiation. The ID provided by the remote unit is used to find the correct certificate to use. If the correct certificate is found, the code then checks that it has been signed by one of the certificate authority certificates (CA*.PEM) that exist on the unit. The code first checks the local certificates, and then the certificate provided by the remote (if any). IKE will send a certificate during negotiations if it is able to find one that has subject “AltName” that matches the ID being used. If not able to locate the certificate, then the remote must have local access to the file so that the public key can be retrieved.

A typical set-up may be that the host unit has a copy of all certificates. This means that the remote units only require the private key, and the certificate authority certificate. This eases administration as any changes to certificates need only be made on the host. Because they do not have a copy of their certificate, remote units rely on the host having a copy of the certificate. An alternative is that the remote units all have a copy of the certificate, as well as the private key and certificate authority certificate, and the host only has its own certificate. This scenario requires that the remote unit send its certificate during negotiations. It can validate the certificate because it has the certificate authority certificate.

FIREWALL SCRIPTS

Introduction

A “firewall” is a protection system designed to prevent access to your local area network by unauthorised “external” parties, i.e. other users of the internet or another wide area network. It may also limit the degree of access local users have to external network resources. A firewall does not provide a complete security solution; it provides only one element of a fully secure system. Consideration should also be given to the use of user authentication and data encryption. Refer to the IPSec section for further information.

In simple terms, a firewall is a packet filtering system that allows or prevents the transmission of data (in either direction) based on a set of rules. These rules can allow filtering based on the following criteria:

- source and destination IP addresses
- source and destination IP port or port ranges
- type of protocol in use
- direction of the data (in or out)
- interface type
- the eroute the packet is on
- if an interface is OOS (out of service)
- ICMP message type
- TCP flags (SYN, ACK, URG, RESET, PUSH, FIN)
- TOS field
- status of a link and/or data packets on UDP/TCP and ICMP protocols

In addition to providing comprehensive filtering facilities, Digi routers also allow you to specify rules relating to the logging of information for audit/debugging purposes. This information can be logged to a pseudo-file on the unit called FWLOG.TXT, the EVENTLOG.TXT pseudo-file or to a syslog server. It can also be used to generate SNMP traps.

Firewall Script Syntax

A firewall must be individually configured to match the needs of authorised users and their applications. On Digi routers the rules governing firewall behaviour are defined in a script file called FW.TXT. Each line in this file consists of a label definition, a comment or a filter rule.

Labels

A label definition is a string of up to 12 characters followed by a colon. Labels can only include letters, digits and the underscore character and are used in conjunction with the break option to cause the processing of the script to jump to a new location.

Comments

Any line starting with the hash character (“#”) is deemed to be a comment and ignored.

Filter Rules

The syntax for a filter rule is:

[action] [in-out] [options] [tos] [proto] [dnslist] [ip-range] [inspect-state]

When the firewall is active, the script is processed one line at a time as each packet is received or transmitted. Even when a packet matches a filter-rule, processing still continues and all the other filter rules are checked until the end of the script is reached. The action taken with respect to a particular packet is that specified by the last matching rule. With the break option however the script processing can be redirected to a new location or to the end of the script if required. The default action that the firewall assigns to a packet is to block. This means that if the packet does not match any of the rules it will be blocked.

The various fields of a script rule are described below:

[action]

The **[action]** field may be specified as **block**, **pass**, **pass-ifup**, **dscp**, **vdscp** or **debug**. These operate as follows:

block

The **block** action prevents a packet from being allowed through the firewall. When block is specified an optional field can be included that will cause an ICMP packet to be returned to the interface from which that packet was received. This technique is sometimes used to confuse hackers by having different responses to different packets or for fooling an attacker into thinking a service is not present on a network.

The syntax for specifying the return of an ICMP packet is:

“return-icmp” [icmp-type [icmp-code]]

where **[icmp_type]** is a decimal number representing the ICMP type or can be one of the predefined text codes listed in the following table:

ICMP type value	ICMP type
1	Unreach
2	Echo
3	Echorep
4	squench
5	redir
6	timex
7	paraprob
8	timest
9	timestrap
10	inforeq
11	inforep
12	maskreg
13	maskrep
14	routerad

ICMP type value	ICMP type
15	routersol

The optional **[icmp-code]** field can also be a decimal number representing the ICMP code of the return ICMP packet but if the **[icmp-type]** is **[unreach]** then the code can also be one of the following pre-defined text codes:

ICMP code	Meaning
net-unr	Network unreachable
host-unr	Host unreachable
proto-unr	Protocol unrecognised
port-unr	Port unreachable
needfrag	Needs fragmentation
srcfail	Source route fail

For example:

```
block return-icmp unreach in break end on ppp 0
```

This rule would cause the unit to return an ICMP Unreachable packet in response to all packets received on PPP 0.

Instead of using the **return-icmp** option to return an ICMP packet, **return-rst** can be used to return a TCP reset packet instead. This would only be applicable for a TCP packet. For example:

```
block return-rst in break end on eth 0 proto tcp from any to 10.1.2.0/24
```

This would return a TCP reset packet when the firewall receives a TCP packet on the Ethernet interface 0 with destination address 10.1.2.*.

pass

The pass action allows packets that match the rule to pass through the firewall.

pass-ifup

The **pass-ifup** action allows outbound packets that match the rule to pass through the firewall but only if the link is already active.

debug

The **debug** action causes the unit to tag any packets matching the rule for debug. This means that for every matching rule that is encountered from this point in the script onwards, an entry will be placed in the pseudo-file FWLOG.TXT.

dscp

The **dscp** action causes any packets matching this rule to have its DSCP value adjusted according to this rule. The DSCP value of a packet indicates the type of service required and is used in conjunction with QOS (Quality of Service) functions. A decimal or hex number must follow the **dscp** keyword to indicate the value that should be set.

vdscp

The **vdscp** action is very similar to the **dscp** action as described above in that it adjusts the DSCP value in a packet. The difference however is that this is a virtual change only which means that the actual packet is not changed, and that the packet is processed as if it had the DSCP value as indicated. Like the dscp action, a decimal or hex number must follow.

[in-out]

The **[in-out]** field can be in or out and is used to specify whether the action applies to inbound or outbound packets. When the field is left blank the rule is applied to any packet irrespective of its direction.

[options]

The **[options]** field is used to define a number of options that may be applied to packets matching the rule. These are:

log

When the **log** option is specified, the unit will place an entry in the FWLOG.TXT file each time it processes a packet that matches the rule. This log will normally detail the rule that was matched along with a summary of the packet contents. If the **log** option is followed by the body sub-option, the complete IP packet is entered into the **log** file so that when the log file is displayed, a more detailed decode of the IP packet is shown.

The **log** field may also be followed by a further sub-option that specifies a different type of log output. This may either be **snmp**, **syslog** or **event**.

If **snmp** is specified an SNMP trap (containing similar information to the normal log entry), is generated when a packet matches the rule.

If **syslog** is specified, a syslog message is sent to the configured syslog manager IP address. This message will contain the same information as that entered into the log file, but in a different format.

If the **body** option has also been specified, some of the IP packet information is also included.

Note that the size of the syslog message is limited to the maximum of 1024 bytes. The syslog message is sent with default priority value of 14, which expands out to facility of USER, and priority INFO.

If **event** is specified the log output will be copied to the EVENTLOG.TXT pseudo-file as well as the FWLOG.TXT file. The event log entry will contain the line number and hit count for the rule that caused the packet to be logged.

Example:

Say your local network is on subnet 192.168.*.* and you want to block any packets received on PPP 0 that were “pretending” to be on the local network and log the receipt of any such packets to the FWLOG.TXT file and to a syslog server. The filter rule would be constructed as follows:

```
block in log syslog break end on ppp 0 from 192.168.0.0/16 to any
```

break

When the **break** option is specified it must be followed by a user-defined label name or the predefined **end** keyword. When followed by a label, the rule processor will “jump” to that label to continue processing. When followed by the **end** keyword rule processing will be terminated and the packet will be treated according to the last matching rule.

Example:

```
break ppp_label on ppp 0
# insert rule processing here for packets that are not on ppp 0
break end
ppp_label
# insert rule processing here for packets that are on ppp 0
```

on

The `on` option is used to specify the interface to which the rule applies and must be followed by a valid interface name. For example, if you were only interested in applying a particular rule to packets being transmitted or received by PPP 0, you would include `on ppp 0` in the rule. Valid interface-names are either `eth n`, `tun n` or `ppp n`, where n is the instance number.

oneroute

The `oneroute` option is used to specify that a rule will only match packets associated with the specified eroute. For example, including the option `oneroute 2` would cause the rule to only match on packets transmitted or received over Eroute 2. The `oneroute` option can be followed with the keyword `any`, which will match if the packet is on any eroute.

routeto

When the `routeto` option is specified and the firewall is processing a received packet, if the rule is the last matching rule, then the packet is tagged as being required to be routed to the specified interface.

For example:

```
pass in break end routeto eth 1 from 10.1.0.0/16 to 1.2.3.4 port=telnet
```

would ensure that all packets from 10.1.*.* to 1.2.3.4 on the telnet port are all routed to ETH 1.

oosed

The `oosed` option is used to check the out of service status of an interface. For example, including the option `oosed ppp 1` would cause the rule to match only if interface PPP 1 is out of service.

[tos]

The `[tos]` field may be used to specify the Type of Service (TOS) to match. If included, the `[tos]` field consists of the keyword `tos` followed by a decimal or hexadecimal code identifying the TOS to match. For example, to block any inbound packet on PPP 0 with a TOS of 0 you would use a rule such as:

```
block in on ppp 0 tos 0
```

[proto]

The `[proto]` field is used to specify a protocol to match and consists of the `proto` keyword followed by one of the following protocol identifiers:

Identifier	Meaning
udp	UDP packet
tcp	TCP packet

Identifier	Meaning
ftp	FTP packets regardless of port number
icmp	ICMP packet
decimal number	decimal number matched to protocol type in IP header

The **[proto]** field is also important when "stateful" inspection is enabled for a rule (using the **[inspect-state]** field), as it describes the protocol to inspect (see **[inspect-state]** below).

[dnslist]

The **[dnslist]** field is used to match packets that contain DNS names that are in a given dnslist. Following **dnslist** there needs to be a name of a dnslist as specified by the **#dns** command. For example, say we have the following dnslist.

```
#dns gglist www.Digi.co.*,www.*.co.nz
```

Then the following firewall rule will block all dns lockups to DNS names matching the above list.

```
block out break end on ppp 1 proto udp dnslist gglist from any to any port=dns
```

[ip-range]

The **[ip-range]** field is used to describe the range of IP addresses and ports to match upon and may be specified in one of several ways. The basic syntax is:

```
ip-range = "all" | "from" ip-object "to" ip-object [flags] [icmp]
```

where **ip-object** is an IP address specification. Full details of the syntax with examples are given under the heading "Specifying IP Addresses and Address Ranges" below.

[inspect-state]

The **[inspect-state]** field is used in create rules for "stateful inspection". This is a powerful option in which the firewall script includes rules that allow the unit to keep track of a TCP/UDP or ICMP session and therefore to only pass packets that match the state of a connection.

Additionally, the **[inspect state]** field can specify an optional OOS (Out Of Service) parameter. This parameter allows the unit to mark any route as being out-of-service for a given period of time in the event that the stateful inspect engine has detected an error.

A full description of how the **[inspect state]** field works is given below under the heading "Stateful Inspection".

Specifying IP Addresses and Ranges

The **ip-range** field of a firewall script rule identifies the IP address or range of addresses to which the rule applies. The syntax for specifying an IP address range is:

```
ip-range = "all" | "from" ip-object "to" ip-object [ flags ] [ icmp ]
```

where:

```
ip-object = addr [port-comp | port-range]
flags = "flags" { flags } [ !{ flags } ]
icmp = "icmp-type" icmp-type [ "code" decnum ]
addr = "any" | ip-addr[ "/"decnum ] [ "mask" ip-addr | "mask" hexnum ]
port-comp = "port" compare port-num
```

```
port-range = “port” port-num “<>” | “><” port-num

ip-addr = IP address in format nnn.nnn.nnn.nnn

decnum = a decimal number

hexnum = a hexadecimal number

compare = “=” | “!=” | “<” | “<=” | “>” | “>=”

port-num = service-name | decnum

service-name = “http” | “telnet” | “ftpdat” | “ftpcnt” | “pop3” | “ike” | “xot”|
“sntp” | “smtp”
```

In the above syntax definition:

- items in quotes are keywords
- items in square brackets are optional
- items in curly braces are optional and can be repeated
- the vertical bar symbol (“|”) means “or”

An **ip-object** therefore consists of an IP address and an IP port specification, preceded by the keyword **from** or **to** to define whether it is the source or destination address. The most basic form for an **ip-object** is simply an IP address preceded by **from** or **to**. For example, to block all packets destined for address 10.1.2.98 the script rule would be:

```
block out from any to 10.1.2.98
```

An **ip-object** can also be specified using an address mask. This is a way of describing which bits of the IP address are relevant when matching. The script processor supports two formats for specifying masks.

Method 1: The IP address is followed by a forward slash and a decimal number. The decimal number specifies the number of significant bits in the IP address. For example, if you wanted to block all packets in the range 10.1.2.* the rule would be:

```
block from any to 10.1.2.0/24
```

i.e. only the first 24 bits of the address are significant.

Method 2: This same rule could be described another way using the mask keyword:

```
block from any to 10.1.2.0 mask 255.255.255.0
```

The IP address can also contain either “**addr-ppp n**” or “**addr-eth n**” where “**n**” is the eth or ppp instance number. In this case the rule is specifying that the IP address is that allocated to the PPP interface or to the Ethernet interface. This is useful in the situation were IP addresses are obtained automatically and therefore are not known by the author of the filtering rules. For example:

```
block in break end on ppp 0 from addr-eth 0 to any
```

Address/Port Translation

One further option that may be used when specifying addresses is to use address translation. The syntax for this is:

```
srcdst = "all | fromto [-> [ip-object] "to" object]
```

I.e. directly after the IP addresses and port are specified an optional "**->**" can follow indicating that the addresses/ports should be translated. The first source object is optional and is unlikely to be used as it is more normal to translate the destination address. The following example will reroute packets originally destined for 10.10.10.12 to 10.1.2.3:

```
pass out break end from any to 10.10.10.12 -> to 10.1.2.3
```

Additionally to this complete subnets can have NAT applied, the address bits not covered by the subnet mask are taken from the original IP address, so for example to NAT the destination subnet of 192.168.0.0/24 to be 192.168.1.0/24 the firewall rule is:

```
pass out break end from any to 192.168.0.0/24 -> to 192.168.1.0/24
```

Filtering on Port Numbers

Now let us say there is a Telnet server running on a machine on IP address 10.1.2.63 and you wish to make this accessible. Using the filter from the previous example would block all packets to 10.1.2.*. To make the Telnet server available on 10.1.2.63 we need to add the following line in front of the blocking rule:

```
pass break end from any to 10.1.2.63 port=23
```

So, a packet being sent to the Telnet server (port 23) on IP address 10.1.2.63 will match this rule and further checking is prevented by the break end option.

The above example illustrates the "=" comparison. Other comparison methods supported are:

Symbol	Meaning
!=	not equal
>	greater than
<	less than
<=	less than or equal to
>=	greater than or equal to

It is also possible to specify a port in range or a port out of range with the "><" or "<>" symbols. For example, to pass all packets to addresses in the range 23 to 28, the rule would be specified as:

```
pass break end from any to 10.1.2.63 port 23><28
```

To simplify references to ports, some commonly used port numbers are associated with the predefined strings listed in the table below. For instance, in the example above we could substitute the number 23 with the string telnet. This would make the rule:

```
pass break end from any to 10.1.2.63 port=telnet
```

The other port keywords that are defined are:

Keyword	Std. Port	Service
Ftpdat	20	File Transfer Protocol data port
Ftpcnt	21	File Transfer Protocol control port

Keyword	Std. Port	Service
telnet	23	Telnet server port
smtp	25	SMTP server port
http	80	Web server port
pop3	110	Mail server port
sntp	123	NTP server port
ike	500	Source/destination port for IKE key
xot	1998	Destination port for XOT packets

Note:
The above service keywords are pre-defined based on “standard” port numbers. It is possible that these may have been defined differently on your system in which case you should use the port numbers explicitly (not the defined names).

Filtering on TCP Flags

An `ip-object` can be followed by an optional `[flags]` field. This field allows the script to filter based on any combination of TCP flags. The `[flags]` field is used to specify the flags to check and consists of the flags keyword followed by a string specifying the flags themselves. Each letter in this string represents a particular flag type as listed below:

Code	Flag
f	FIN Flag
r	RESET Flag
s	SYN Flag
p	PUSH Flag
u	URG Flag
a	ACK Flag

These flag codes allow the filter to check any combination of flags.

Following on from the previous example, to block packets that have all the flags set you would need to precede the pass rule with the following block rule:

```
block break end from any to 10.1.2.0/24 port=telnet flags frspua
```

Here, the list of flags causes the unit to check that those flags are set. This list may be optionally followed by an exclamation mark (“!”) and a second list of flags that the unit should check for being clear.

For example:

```
flags s!a
```

would test for the `s` flag being on and the `a` flag being off with all other flags ignored.

As a further example, let us say we want to allow outward connections from a machine on 10.1.2.33 to a Telnet server. We have to define a filter rule to pass outbound connections and the inbound response packets. Because this is an outbound Telnet service we can make use of the fact that all incoming packets will have their ACK bits set. Only the first packet establishing the connection will have the ACK bit off. The filter rules to do this would look like this:

```
pass out break end from 10.1.2.33 port>1023 to any port=telnet

pass in break end from any port=telnet to 10.1.2.33 port>1023 flags !a
```

The first rule allows the outward connections, and the second rule allows the response packets back in which the ACK flag must always be on. This second rule will filter out any packets that do not have the ACK flag on. This will bar any attackers from trying to open connections onto the private network by simply specifying the source port as the Telnet port (note that there is a simpler way to achieve the same effect using the inspect state option described below).

Filtering on ICMP Codes

An **ip-object** can be followed by an optional **[icmp]** field. This allows the script to filter packets based on ICMP codes. ICMP packets are normally used to debug and diagnose a network and can be extremely useful. However they form part of a low-level protocol and are frequently exploited by hackers for attacking networks. For this reason most network administrators will want to restrict the use of ICMP packets.

The syntax for including ICMP filtering is:

```
icmp = “icmp-type” icmp-type [“code” decnum]
```

The **icmp-type** can be one of the pre-defined strings listed in the following table or the equivalent decimal numeric value:

ICMP Type	ICMP Value
Unreach	3
Echo	8
Echorep	0
Squench	4
Redir	5
Timex	11
Paramprob	12
Timest	13
Timestrep	14
Inforeq	15
Inforep	16
Maskreq	17
Maskrep	18
Routerad	9
Routersol	10

The following two rules are therefore equivalent:

```
pass in break end on ppp 0 proto icmp from any to 10.1.2.0/24 icmp-type 0
pass in break end on ppp 0 proto icmp from any to 10.1.2.0/24 icmp-type echorep
```

Both of these rules allow echo replies to come in from interface `ppp 0` if they are addressed to our example local network address (10.1.2.*).

In addition to having a type, ICMP packets also include an ICMP code field. The filter syntax allows for the specification of an optional code field after the ICMP type. When specified the code field must also match. The ICMP code field is specified with a decimal number.

For example, suppose we wish to allow only echo replies and ICMP unreachable type ICMP packets from interface PPP 0. Then the rules would look something like this:

```
pass in break end on ppp 0 proto icmp from any to 10.1.2.0/24 icmp-type echorep code 0
pass in break end on ppp 0 proto icmp from any to 10.1.2.0/24 icmp-type unreach code 0
block in break end on ppp 0 proto icmp
```

The first two rules in this set allow in the ICMP packets that we are willing to permit and the third rule denies all other ICMP packets in from this interface. Now if we ever expect to see echo replies in on `ppp 0` we should allow echo requests out on that interface too. To do that we would have the rule:

```
pass out break end on ppp 0 proto icmp icmp-type echo
```

Stateful Inspection

The Digi routing code stack contains a sophisticated scripted “Stateful Firewall” and “Route Inspection” engine. Stateful inspection is a powerful tool that allows the unit to keep track of a TCP/UDP or ICMP session and match packets based on the state of the connection on which they are being carried. In addition to providing sophisticated Firewall functionality the SF/RI engine also provides a number of facilities for tracking the “health” of routes, marking “dead” routes as being Out Of Service (OOS) and creating rules for the automatic status checking of routes previously marked as OOS (for use in multilevel backup/restore scenarios).

The firewall may be used to place interface into an OOS state and also control how the interfaces return to service. When an interface goes OOS, all routes configured to use that interface will have their route metric set to 16 (the maximum value), meaning that some other route with a lower metric will be selected.

When a firewall stateful inspection rule expires, a decision is made as to whether the traffic being allowed to pass by this rule completed successfully or not. For example, if the stateful rule monitors SYN and FIN packets in both directions for a TCP socket then that rule will expire successfully. However, if SYNs are seen to pass in one direction but no SYNs pass in the other direction, the stateful rule will expire and the unit will tag this as a failure.

The following conditions tag a stateful rule as a failure:

• packets have only passed in one direction

• 10 packets have passed in one direction with no return packets (for TCP the packets must also be re-transmits) All of these features depend upon the stateful inspection capabilities of the Firewall engine which are explained below.

The `[inspect]` field takes the following format:

```
inspect = [“inspect-state” {“oos” {interface-name¦logical-name} secs {t=secs}
{c=count} {d=count}} {r=“ping”¦“tcp”{,secs{secs}}} {rd=x} {dt=secs}{stat}]
```

The field can be used on its own or with an optional **oos** (Out Of Service) parameter.

To understand this better let us look at a simple example in which we want to set up a filter to allow all machines on a local network with addresses in the range 10.1.2.*, to access the Internet on port 80. We will need one rule to filter the outgoing packets and another to filter the responses:

```
pass out break end on ppp 0 from 10.1.2.0/24 to any port=80

pass in break end on ppp 0 from any port=80 to 10.1.2.0/24
```

In this example, the first rule allows outgoing http requests on PPP 0 from any address matching the mask 10.1.2.* providing that the requests are on port 80 (the normal port address for HTTP requests).

The second rule allows http response packets to be received on PPP 0 providing they are on port 80 and they are addressed to an IP address matching the mask 10.1.2.*.

However, rule 2 creates a potential security “hole”. The problem with filtering based on the source port is that you can trust the source port only as much as you trust the source machine. For instance an attacker could perform a port scan and provided the source port was set to 80 in each packet, it would get through this filter. Alternatively, on an already compromised system, a “Trojan horse” might be set up listening on port 80.

A more secure firewall can be defined using the “inspect-state” option. The stateful inspection system intelligently creates and manages dynamic filter rules based on the type of connection and the source/destination IP addresses. Applying this to the above example, we can redesign the script to make it both simpler and more effective as described below.

As a consequence of the fact that only the first packet in a TCP handshake will have the SYN flag set, we can use a rule that checks the SYN flag:

```
pass out break end on ppp 0 from 10.1.2.0/24 to any port=80 flags s inspect-state

block in break end on ppp 0
```

The first rule matches only the first outgoing packet because it checks the status of the s (SYN) flag and will only pass the packet if the SYN flag is set. At first glance however, it appears that the second rule blocks all inbound packets on PPP 0. Whilst this may be inherently more secure, it would also mean that users on the network would not be able to receive responses to their HTTP requests and would therefore be of little use!

The reason that this is not a problem is that the stateful inspection system creates temporary filter rules based on the outbound traffic. The first of these temporary rules allows the first response packet to pass because it also will have the SYN flag set. However, once the connection is established, a second temporary rule is created that passes inbound or outbound packets if the IP address and port number match those of the initial rule but does not check the SYN flag. It does however monitor the FIN flag so that the system can tell when the connection has been terminated. Once an outbound packet with the FIN flag has been detected along with a FIN/ACK response, the temporary rule ceases to exist and further packets on that IP address/port are blocked.

In the above example, if a local user on address 10.1.2.34 issues an http request to a host on 100.12.2.9, the outward packet would match and be passed. At the same time a temporary filter rule is automatically created by the firewall that will pass inbound packets from IP address 100.12.2.9 that are addressed to 10.2.1.34 port x (where x is the source port used in the original request from 10.1.2.34).

This use of dynamic filters is more secure because both the source and destination IP addresses/ports are checked. In addition, the firewall will automatically check that the correct flags are being used for each stage of the communication.

The potential for a security breach has now been virtually eliminated because even if a hacker could time his attack perfectly he would still have to forge a response packet using the correct source address and port (which was randomly created by the sender of the HTTP request) and also has to target the specific IP address that opened the connection.

Another advantage of "**inspect-state**" rules is that they are scalable, i.e. many machines can use the rule simultaneously. In our above example for instance many machines on the local network could all browse the Internet and the inspection engine would be dynamically creating precise inward filters as they are required and closing them when they are finished with.

The **inspect-state** option can be used on TCP, UDP protocols and some ICMP packets. The ICMP types that can be used with the "**inspect-state**" option are "**echo**", "**timest**", "**inforeq**" and "**maskreq**".

Using [inspect-state] with Flags

As can be seen above, the **inspect-state** option can be used with flags. To illustrate this we will refer back to the earlier example of filtering using flags. It is possible to simplify the script by using the **inspect-state** option. The original script was:

```
pass out break end from 10.1.2.33 port>1023 to any port=telnet
pass in break end from any port=telnet to 10.1.2.33 port>1023 flags a!
```

Using the inspect state option this can be replaced with a single filter rule:

```
pass out break end from 10.1.2.33 port>1023 to any port=telnet flags s!a inspect-state
```

No rule is needed for the return packets because a temporary filter will be created that will only allow inbound packets to pass if they match sessions set up by this stateful inspection rule.

A further point to note about the new rule is that the "**flags s!a**" specification ensures that it only matches the first packet in a connection. This is because the first packet in a TCP connection has the SYN flag on and the ACK flag off and so we only match on that combination. The stateful inspection engine will take care of matching the rest of the packets for this connection.

Using [inspect-state] with ICMP

The **[inspect-state]** option can be also used with ICMP codes. To allow the use of echo request and to allow echo replies you would have just the one rule:

```
pass out break end on ppp 0 proto icmp icmp-type echo inspect-state
```

The advantage of using **inspect-state**, other than just needing one rule, is that it leads to a more secure firewall. For instance with the **inspect-state** option the echo replies are not allowed in all the time; they will only be allowed in once an echo request has been sent out on that interface. The moment that a valid echo reply comes back (or there is a timeout), echo replies will again be blocked. Furthermore, the full IP address is checked; the IP source and destination must exactly match the IP destination and source of the echo request. If you compare this to the rule to allow echo replies in without using **inspect-state** it would not be possible to check the source address at all and the destination address would match any IP address on our network.

The **inspect-state** option can be used with the following ICMP packet types:

ICMP Type	Matching ICMP Type
Echo	Echo reply
Timest	Timestrep
Inforeq	Inforep
Maskreq	Maskrep

Using [inspect-state] with the Out Of Service Option

The **inspect-state** field can be used with an optional **oos** parameter. This parameter allows the stateful inspect engine to mark as "out of service" any routes that are associated with the specified interface and also to control how and the interfaces are returned to service. Such routes will only be marked as out of service if the specified oos option parameters are met. The **oos** parameter takes the format:

```
oos {interface-name¦logical-name} secs {t=secs} {c=count} {d=count}
{r="ping"|"tcp"{,secs}}
```

where:

interface-name or **logical-name** specifies the interface with which the firewall rule is associated, e.g. PPP 1. This can also be a logical interface name which is simply a name that can be created (e.g. "waffle"). When a logical interface name is specified then this name can become oos (out of service) and can be tested in other firewall rules with the **oosed** keyword.

secs specifies the length of time in seconds for which the routes that are using the specified interface are marked as out of service.

{t=secs} is an optional parameter that specifies the length of time in seconds the unit will wait for a response the packet that matched the rule.

{c=count} is an optional parameter that specifies the number of times that the stateful inspection engine must trigger on the rule before the route is marked as out of service.

{d=count} is an optional parameter that specifies the number of times that the stateful inspection engine must trigger on the rule before the interface is deactivated (only applies to PPP interfaces).

{r="ping"|"tcp"{,secs{,secs}}} is an optional parameter that specifies a recovery procedure. When a recovery procedure is specified then after the oos timeout has expired instead of bringing the interface back into service immediately the link is tested first. It is tested by either sending a TCP SYN packet or a ping packet to the address/port that caused the oos condition. The "secs" field specifies the retry time when checking for recovery. Only when the recovery succeeds will interface become in service again.

UDP Example

```
pass in

pass out

pass out on ppp 1 proto udp from any to 156.15.0.0/16 port=1234 inspect-state oos ppp
1 300 t=10 c=2 d=2
```

The first two rules simply configure the unit to allow any type of packets to be transmitted or received (the default action of the firewall is to block all traffic).

The third rule is more complex. What it does is to configure the stateful inspection engine to watch for UDP packets (with any source address) being routed via the PPP 1 interface to any address that begins with 156.15 on port 1234. If a hit occurs on this rule but the unit does not detect a reply within 10 seconds (as specified by the **t=** parameter), it will increment an internal counter. When this counter reaches the value set by the **c=** parameter, the stateful inspection engine will mark the PPP 1 interface (and therefore any routes using it), as being out of service for 300 seconds. Similarly, if this counter matches the **d=** parameter the stateful inspection engine will deactivate PPP 1. So in the above example, the stateful inspection engine will mark any routes that use PPP 1 as out of service AND deactivate PPP 1 if no reply is detected within 10 seconds for two packets in a row.

Routes will come back into service when either the specified timeout expires or if there are no other routes with a higher metric in service.

PPP interfaces will be re-activated when either the routes using them are back in service and there is a packet to route and the AODI mode parameter is set to “On”.

TCP Example

```
pass out log break end on ppp 3 proto tcp from any to 192.168.0.1 flags S!A inspect-state oos 30 t=10 c=2 d=2

pass in

pass out
```

This rule will specifically trace attempts to open a TCP connection on PPP 3 to the 192.168.0.1 IP address and if it fails within 10 seconds twice in a row, will cause the PPP 3 interface to be flagged as out of service (i.e. its metric will be set to 16), for 30 seconds. The optional **d=2** entry will also cause the PPP link to be deactivated. Deactivating the link can be useful in scenarios where renegotiating the PPP connection is likely to resolve the problem. Again, if a matching route with a higher metric has been defined it will be used whilst PPP 3 routes are out of service thus providing a powerful route backup mechanism.

Using [inspect-state] with the Stat Option

The **inspect-state** option can be used with the **stat** option. The **stat** option will cause this firewall rule to record statistics associated with this firewall rule. Transaction times, counts and errors are recorded under the PPP statistics with this option.

Assigning DSCP Values

When using QOS, packet priorities will be determined by the DSCP values in their TOS fields. These priorities may have already been assigned but if necessary, the router can be configured to assign them by inserting the appropriate rules in the firewall. This is done by using the **dscp** command.

For example:

```
dscp 46 in on eth 0 from 100.100.100.25 to 1.2.3.4 port=4000
```

would set the DSCP value to 46 for almost any type of packet received on ETH 0 from IP address 100.100.100.25 addressed to 1.2.3.4 on port 4000. This allows you to set the DSCP value for almost any type of packet.

As a further example:

```
dscp 46 in on eth 0 proto smtp from any to any
```

would cause outgoing mail traffic to the same top priority queue (46 is by default a very high priority code in the DSCP mappings).

The FWLOG.TXT File

When the log option is specified within a firewall script rule, an entry is created in the FWLOG.TXT pseudo-file each time an IP packet matches the rule. Each log entry will in turn contain the following information:

Parameter	Description
Timestamp	The time when the log entry is created.
Short Description	Usually “FW LOG” but could be “FW DEBUG” for packets that hit rules with the “debug” action set.
Dir	Either “IN” or “OUT”. Indicates the direction the packet is travelling.
Line	The line number of the rule that cause the packet to be logged.
Hits	The number of matches for the rule that caused this packet to be logged.
Iface	The Interface the packet was to be transmitted/received on.
Source IP	The source IP address in the IP packet.
Dest. IP	The destination IP address in the IP packet.
ID	The value of the ID field in the IP packet.
TTL	The value of the TTL field in the IP packet.
PROTO	The value of the protocol field in the IP packet. This will be expanded to text as well for the well-known protocols.
Src Port	The value of the source port field in the TCP/UDP header.
Dst Port	The value of the source port field in the TCP/UDP header.
Rule Text	The rule that caused the packet to be logged is also entered into the log file.

In addition, port numbers will be expanded to text pre-defined port numbers.

Log File Examples

Example: log entry **without** the **body** option:

```
----- 15-8-2002 16:25:50 ------
FW LOG Dir: IN Line: 11 Hits: 1 IFACE: ETH 0
Source IP: 100.100.100.25 Dest IP: 100.100.100.50 ID: 39311 TTL: 128
PROTO: TCP (6)
Src Port: 4232 Dst Port: WEB (80)
pass in log break end on eth 0 proto tcp from 100.100.100.25 to addr-
eth 0
flags S/SA inspect-state
----------
```

Example: Log entry **with** the **body** option:

```
----- 15-8-2002 16:27:56 ------
FW LOG Dir: IN Line: 7 Hits: 1 IFACE: ETH 0
Source IP: 100.100.100.25 Dest IP: 100.100.100.50 ID: 40140 TTL: 128
PROTO: ICMP (1)
```

```
block return-icmp echorep log body break end proto icmp icmp-type echo
From REM TO LOCIFACE: ETH 0
45 IP Ver: 4
Hdr Len: 20
00 TOS: Routine
Delay: Normal
Throughput: Normal
Reliability: Normal
00 3C Length: 60
9C CC ID: 40140
00 00 Frag Offset: 0
Congestion: Normal
May Fragment
Last Fragment
80 TTL: 128
01 Proto: ICMP
0C E1 Checksum: 3297
64 64 64 19 Src IP: 100.100.100.25
64 64 64 32 Dst IP: 100.100.100.50
ICMP:
08 Type: ECHO REQ
00 Code: 0
04 5C Checksum: 1116
----------
```

Example: Text included in the EVENTLOG.TXT pseudo-file when the **event** sub-option is specified:

```
16:26:32, 15 Aug 2002,Firewall Log Event: Line: 10, Hits: 3
```

Example: Syslog message where the **body** option is **not** specified:

```
2002-09-04 16:30:06 User.Info100.100.100.50Aug 15 16:31:59 arm.1140
IP Filter -
Filter Rule: block return-icmp unreach host-unr in log syslog break
end on eth 0 proto tcp from any to 100.100.100.50 port=telnet
Line: 10
Hits: 4
```

Example: Syslog message with the **body** option **is** specified:

```
2002-08-30 16:19:59 User.Info100.100.100.50Aug 10 16:21:56 arm.1140
IP Filter - Filter Rule: block return-icmp unreach port-unr in log
body syslog break end on eth 0 proto tcp from any to 100.100.100.50
port=telnet
Line: 9
Hits: 3
PKT:
Source IP: 100.100.100.25
Dest IP: 100.100.100.50
ID: 13317
TTL: 128
Protocol: TCP
Source Port: 1441
```

```
Dest Port: 23
TCP Flags: S
```

Further [inspect-state] Examples

Here is a basic **inspect-state** rule with no OOS options:

```
pass out break end on PPP 2 proto TCP from 10.1.1.1 to 10.1.2.1 port=telnet flags S!A
inspect-state
```

This rule will allow TCP packets from 10.1.1.1 to 10.1.2.1 port 23 with the SYN flag set to pass out on PPP 2. Because the **inspect-state** option is used, a stateful rule will also be set up which allows other packets for that TCP socket to also pass.

Next, we will modify the rule to mark an interface OOS if a stateful rule identifies a failed connection:

```
pass out break end on PPP 2 proto TCP from 10.1.1.1 to 10.1.2.1 port=telnet flags S!A
inspect-state oos 60
```

The addition of **oos 60** means that if the stateful rule sees a failure, interface PPP 2 will be set OOS for 60 seconds. If no interface is specified after the **oos** keyword, the interface set to OOS will be the one the packet is currently passing on. It is possible to OOS a different interface by specifying the interface after the **oos** keyword, e.g. **oos ppp 1 60** to put PPP 1 out of service for 60 seconds.

The default time allowed by the stateful rule for a connection to open may be overridden by using the **{t=secs}** option. E.g. To override the default TCP opening time of 60 seconds to 10 seconds:

```
pass out break end on PPP 2 proto TCP from 10.1.1.1 to 10.1.2.1 port=telnet flags S!A
inspect-state oos 60 t=10
```

A socket will now only have 10 seconds to become established (i.e. exchange SYNs) before the stateful rule will expire and be tagged as a failure.

It is possible to configure the firewall so that the interface is only set to OOS after a number of consecutive failures occur. To do this, use the **{c=count}** option. For example:

```
pass out break end on PPP 2 proto TCP from 10.1.1.1 to 10.1.2.1 port=telnet flags S!A
inspect-state oos 60 t=10 c=5
```

PPP 2 will now only be set OOS after 5 consecutive failures.

It is possible to deactivate the interface after a number of consecutive failures. This is useful for WWAN interfaces, which may get into a state where the PPP connection appears to be operational, but in fact no packets are passing. In this case, deactivating and reactivating the interface will sometimes fix the problem.

For example:

```
pass out break end on PPP 2 proto TCP from 10.1.1.1 to 10.1.2.1 port=telnet flags S!A
inspect-state oos 60 t=10 c=5 d=10
```

Now, PPP 2 will be deactivated after 10 consecutive failures.

Keeping a route out of service and using recovery

It may be that the user wants to keep the interface OOS until he is sure that a future connection will work. To help achieve this, one or more recovery options may be specified. These options get the unit to test connectivity between the unit and the destination IP address of the packet that established the stateful rule. The recovery can be in the form of a PING or a TCP socket connection. An interval between recovery checks must also be specified. For example:

```
pass out break end on PPP 2 proto TCP from 10.1.1.1 to 10.1.2.1 port=telnet flags S!A
inspect-state oos 60 t=10 c=5 d=10 r=tcp,120
```

Now the interface will be set to OOS for 60 seconds after 5 consecutive failures. After the 60 seconds elapses, the recovery procedure will be initiated. In this example the recovery will consist of TCP connection attempts executed at 2 minute intervals. The interface will remain OOS until the recovery procedure completes successfully. The destination IP address in this case will be 10.1.2.1.

To override the default socket connection time, it is possible to specify an additional recovery option. For example:

```
pass out break end on PPP 2 proto TCP from 10.1.1.1 to 10.1.2.1 port=telnet flags S!A
inspect-state oos 60 t=10 c=5 d=10 r=tcp,120,10
```

Now, 10 seconds is allowed for each recovery attempt. If the socket connects within that time, the recovery is successful, else the recovery is unsuccessful.

There is also an option **{rd=x}** to disconnect the interface after a recovery attempt completes. This option can be used to deactivate the interface after a recovery failure, success, or either. "**x**" is a bitmask indicating the cases where the interface should be deactivated. Bit 0 is used to deactivate the interface after a recovery failure. Bit one is used to deactivate the interface after a recovery success, i.e.

- rd=1 – means deactivate after a recovery failure
- rd=2 – means deactivate after a recovery success
- rd=3 – means deactivate after either recovery success or recovery failure

Extending our firewall rule to include this option gives:

```
pass out break end on PPP 2 proto TCP from 10.1.1.1 to 10.1.2.1 port=telnet flags S!A
inspect-state oos 60 t=10 c=5 d=10 r=tcp,120,10 rd=3
```

Now the interface will be deactivated after a recovery success or failure.

If the **{rd=x}** option is not used, the interface will remain up until its inactivity timer expires, or it is deactivated by some other means.

The **{dt=secs}** option may be used to indicate that the interface is to remain OOS when it is disconnected, and that it should be reactivated some time after it last disconnected. Recovery procedures will take place after the interface connects.

Extending our firewall rule to include this option gives:

```
pass out break end on PPP 2 proto TCP from 10.1.1.1 to 10.1.2.1 port=telnet flags S!A
inspect-state oos 60 t=10 c=5 d=10 r=tcp,120,10 rd=3 dt=60
```

Now the interface will be reconnected 60 seconds after it disconnects and recovery procedures will start after the interface connects. This option would normally be used with the **{rd=x}** option so that recovery has control over when the interface connects and disconnects.

Keeping a route out of service and using recovery with a list of addresses

This expands on the functionality above and gives the ability to check connectivity to a range of addresses using a ping. It is possible to specify an address list that the recovery mechanism will ping in turn to see if any respond. This will help ensure that even when 1 or maybe 2 or 3 destinations cant be reached due to an outage on the remote network, the connection will be made available again if at least one of the addresses in the list responds.

The address lists are created using the following syntax:

```
#addrs <list-name> <address1,address2,address3,address4>
```

Address lists can span multiple lines if required, for example:

```
#addrs <list-name> <address1,address2>
#addrs <list-name> <address3,address4>
```

The address list is called using the recovery option pingl. An example firewall rule would be:

```
pass out break end on PPP 1 proto ICMP from 10.1.1.1 to 10.1.2.1 inspect-state oos 60
t=10 c=5 d=10 r=pingl listA ,120,10 rd=3 dt=60
```

This rule would allow pings outbound and on detecting a communication failure it will use pings to a address list named listA. The address list named listA could look like this:

```
#addrs listA 10.1.2.1,10.1.3.1,10.1.4.1,10.1.5.1
#addrs listA 10.1.6.1,10.2.1.1,10.2.2.1
```

This causes the recovery to ping the range of address shown in the list above.

Debugging a Firewall

During the creation and management of firewall scripts, firewall scripts may need debugging to ensure that packets are being processed correctly. To assist in this, a rule with the debug action may be used.

If a rule with the **debug** action is encountered, an entry is made in the FWLOG.TXT pseudo-file each time the packet in question matches a rule from that point on. This gives the administrator the ability to follow a packet through a rule set, and can help determine what, if any, changes are required to the rule set. Rules that specify the **debug** action would typically be placed near the top of the rule set, so that all matching rules from that point on are entered into the log file.

Entries the FWLOG.TXT file created as the result of a **debug** rule may be identified by the short description “FW_DEBUG” at the top of the log entry.

An example rule set using a **debug** rule:

```
debug in on ppp 2 proto tcp from any to any port=http
pass in break end proto tcp from any to any port=http flags s/sa inspect state
pass out break end proto udp
```

If placed at the top of the rule set, any packet received on interface PPP 2 to destination port 80 will generate a debug entry in the log file for each subsequent rule that it matches. In the example rule set above, a packet that matched the second rule would also match the first rule, and would therefore create two log entries. The same packet would not match the third rule, and so no log entry would be made for this rule.

Because of the extra processor time required to add all of these additional log entries, debug rules should be removed (or commented out) once the rule set is operating as desired.

REMOTE MANAGEMENT

Digi products equipped with ISDN BRIs can be accessed and controlled remotely via the ISDN network by using:

- a V.120 connection to access the text command interface
- PPP to access the Web Interface
- PPP to access the text command interface using Telnet
- the X.25 remote command channel

Remote access via any one of these methods can be used to reconfigure the unit, upload/download files or upgrade the software, examine the event log or protocol analyser traces or to view statistics.

Using V.120

To establish a remote access session using V.120, initiate a V.120 call as normal using the ATD command. Enter "%%%" within 5 seconds of the remote unit answering and you will be prompted to enter your username and password. Correct entry of these will allow access to the text command interface. If the remote unit has been programmed with a **Router Identity** string on the ***Configuration - System > Device Identity*** page, the **Router Identity** will appear as the command line prompt. Three login attempts are permitted before the connection is reset.

Using Telnet

If you have created a PPP DUN (Dial-up Networking) entry for the remote unit that you wish to access, any terminal program that supports Telnet may be used to establish a remote connection.

To initiate the connection, launch the DUN. If the remote unit is configured correctly with one of the PPP instances enabled for answering, it will connect and the linked computers icon will appear in the Windows system tray. You may then load your Telnet software.

To configure your Telnet software you must first specify that you require a TCP/IP connection and then enter the appropriate IP address or hostname (e.g. 1.2.3.4, 192.168.1.1 or digi.router by default). After ensuring that your software is configured to connect to TCP port number 23 you may then initiate a new connection.

If the connection is successful you will see a connect confirmation message and you will be prompted to enter your username and password. Correct entry of these will allow access to the text command interface. If the remote unit has been programmed with a **Router Identity** string on the ***Configuration - System > Device Identity*** page the **Router Identity** will appear as the command line prompt.

Three login attempts are permitted before the connection is reset.

Using FTP

TransPort routers incorporate an FTP server. FTP allows users to log on to remote hosts for the purpose of inspecting file directories, retrieving or uploading files, etc. For PC users, MS-DOS includes FTP support and there are a number of Windows-based specialist FTP client programs such as CuteFTP™ and Ws_ftp™. Many browsers also incorporate FTP support.

To initiate remote access to a unit using FTP, first establish a PPP DUN connection to the unit and then run your FTP software.

Note:
If your unit has a USB storage device attached, it will show up as a sub-folder named “usb”.

FTP under Windows

Once the connection has been established, enter the Web address for the unit. By default this will be:

1.2.3.4, 192.168.1.1 or digi.router

If you are using a browser, as opposed to a specific FTP program, you will need to precede the address with “ftp://”. For example:

ftp://digi.router

This will give you an anonymous FTP login to the remote unit and you should see a listing of the file directory (the format of this will depend on the FTP client software that you are using). With an anonymous login you will be able to view and retrieve files, but NOT upload, rename or delete them.

For full file access, you will need to log in with your correct username and password. To do this, enter the address in the following format:

ftp://username:password@digi.router

This will give you full access and will allow you to copy, delete, rename, view and transfer files.

When using a browser CUT, COPY, DELETE and PASTE may be used for manipulating files as if they were in a normal Windows directory. If you are using a specific FTP client program, these operations may be carried out using menu options or buttons.

FTP under DOS

To use FTP under DOS, use Windows DUN to establish the connection and then run the MSDOS prompt program. At the DOS prompt type:

ftp digi.router

or

ftp 192.168.1.1

When the connection has been established you will be prompted to enter your username and password. Following a valid login the ftp> prompt will be issued and you may proceed to use the various ftp commands as appropriate. To obtain a list of available commands enter “?” at the prompt.

Using X.25

Remote access to your unit may also be carried out over an X.25 connection. The remote unit must first have the parameter **Allow CLI access from X.25 address** set to an appropriate value (see ***Configuration - System > General***). If the unit then receives an incoming X.25 call where the trailing digits of the NUA match the specified sub-address, the calling user will receive the standard login prompt. On entry of a valid username and password, they will be given access to the command line as if they were connected locally.

AT COMMANDS

D Dial

The ATD command causes the unit to initiate an ISDN call. The format of the command depends on the mode of operation.

When using the unit to make data calls on one of the ISDN B-channels, enter the ATD command followed by the telephone number. For example, to dial 01234 567890 enter the command:

atd01234567890

Spaces in the number are ignored. If the call is successful the unit will issue the CONNECT result code and switch to on-line mode.

Dialling with a Specified Sub-Address

The ATD command may also be used to route a call to an ISDN sub-address by following the telephone with the letter S and the required sub-address. The sub-address may be up to 15 digits long. For example:

atd01234567890s003

Dialling Stored Numbers

To dial numbers that have previously been stored within the unit using the AT&Z command, insert the S= modifier within the dial string. For example, to dial stored number 3 use the command:

atds=3

Combining ISDN and X.25 Calls

A further option for the ATD command for X.25 applications is to combine the ISDN call and the subsequent X.25 CALL in the same command. To do this, follow the telephone number with the "=" symbol and the X.25 call string. For example:

atd01234 567890=123456789

Pressing any key while the ATD command is being executed will abort the call attempt.

H Hang-up

The ATH command is used to terminate an ISDN call. If the unit is still on-line you must first switch back to command mode by entering the escape sequence, i.e. +++, wait 1 second and then enter an AT command or just AT<CR>.

After entering the ATH command the call will be disconnected and the NO CARRIER result will be issued.

Z Reset

The ATZ command is used to load one of the stored profiles for the active ASY port. The command is issued in the format ATZn where n is the number (0 or 1) of the ASY port profile you wish to load.

&C DCD Control

The AT&C command is used to configure the way in which the unit controls the DCD signal to the terminal. There are three options:

&C0 DCD is always On

&C1 DCD is On only when an ISDN connection has been established (Layer 2 is UP)

&C2 DCD is always Off

&C3 DCD is normally On but pulses low for a time in 10 msec units determined by S register 10.

&F Load Factory Settings

The AT&F command is used to load a pre-defined default set of S-register and AT command settings (the default profile). These are:

E1, V1, &C1, &K1, &D2, S0=0, S2=43

All other values are set to 0.

&R CTS Control

The AT&R command is used to configure the way in which the unit controls the CTS signal to the terminal. There are three options:

&R0 CTS is always On

&R1 CTS follows RTS. The delay between RTS changing and CTS changing is set in AT register 56 in multiples of 10msec

&R2 CTS is always Off

&V View Profiles

The AT&V command displays a list of the current AT command and S register values, and the settings for the two stored profiles. For example:

```
at&v
CURRENT PROFILE:
&c1 &d2 &k1 &s1 &r0 e1 q0 v1 &y0
S0=0 S2=43 S12=50 S31=3 S45=5
states DTR:1 RTS:1

STORED PROFILE 0:
&c1 &d2 &k1 &s1 &r0 e1 q0 v1
S0=0 S2=43 S12=50 S31=3 S45=5

STORED PROFILE 1:
&c1 &d2 &k1 &s1 &r0 e1 q0 v1
S0=0 S2=43 S12=50 S31=3 S45=5
OK
```

&W Write SREGS.DAT

The AT&W command is used to save the current command and S registers settings (for the active port), to the file SREGS.DAT. The settings contained in this file can be reloaded at any time using the ATZ command.

The AT&W command may be immediately followed by a profile number, either 0 or 1, to store the settings in the specified profile, for example:

at&w1

would store the current settings as profile 1. If no profile number is specified, profile 0 is assumed.

All S register values and the following command settings are written by AT&W:

e, &c, &d, &k

&Y Set Default Profile

The AT&Y command is used to select the power-up profile (0 or 1). For example, to ensure that the unit boots up using stored profile 1, enter the command:

at&y1

&Z Store Phone Number

The AT&Z command is used to store “default” telephone numbers within the unit that may subsequently dialled when DTR dialling is enabled or by using the S= modifier in the ATD dial command. One telephone number may be stored for each ASY port. For example, to store the phone number 0800 123456 as the default number to be associated with ASY 2, use the command:

at&z2=0800123456

If the number of the ASY port is not specified, the number will be stored against the port from which the command was entered, i.e. entering the command:

at&z=0800123456

from ASY 3 has the same effect as:

at&z3=0800123456

from any port. Once a number has been stored it may be dialled from the command line using the ATD command with the S= modifier:

atds=3

This means that any stored number can be dialled from any port. If DTR dialling has been enabled by setting S33=1 for the port, the number associated with that port will be dialled when the DTR signal for that port changes from Off to On, i.e. DTR dialling can only be used with the number associated with the port to which the terminal is connected.

\AT Ignore Invalid AT Commands

This command is a work-around for use with terminals that generate large amounts of extraneous text. If not ignored, this text can cause many error messages to be generated by the router, and may result in a communications failure. To turn on this feature, type the following command:

at\at=1

To turn off the feature, type the following command:

at\at=0

When this feature is turned on, the ASY port ignores all commands except real AT commands. As with other ASY modes this can be saved by AT&W but is not included in the AT&V status display. To determine whether or not this mode is enabled type:

at\at ?

The unit will display 0 if the feature is Off, 1 if it is On.

\LS Lock Speed

The AT\LS command is used to lock the speed and data format of the port at which it is entered to the current settings so that the non-AT application commands may be used.

\PORT Set Active Port

Text commands which affect the settings associated with the serial ports normally operate on the port at which they are entered, i.e. entering the AT&K command from a terminal connected to ASY 1 will affect only the flow control settings for port 1.

The AT\PORT command is used to select a different “active” port from that at which the commands are entered. For example, if your terminal is connected to port 0 and you need to reconfigure the settings for port 2, you would first enter the command:

at\port=2
PORT 2
OK

Port 2 is now the active port and any AT commands or changes to S registers settings which affect the serial ports will now be applied to port 2 only. This includes:

Commands: Z, &D, &F, &K, &V, &Y, &W

S registers: S31, S45

The AT\PORT? command will display the port to which you are connected and the active port for command/ S register settings. For example:

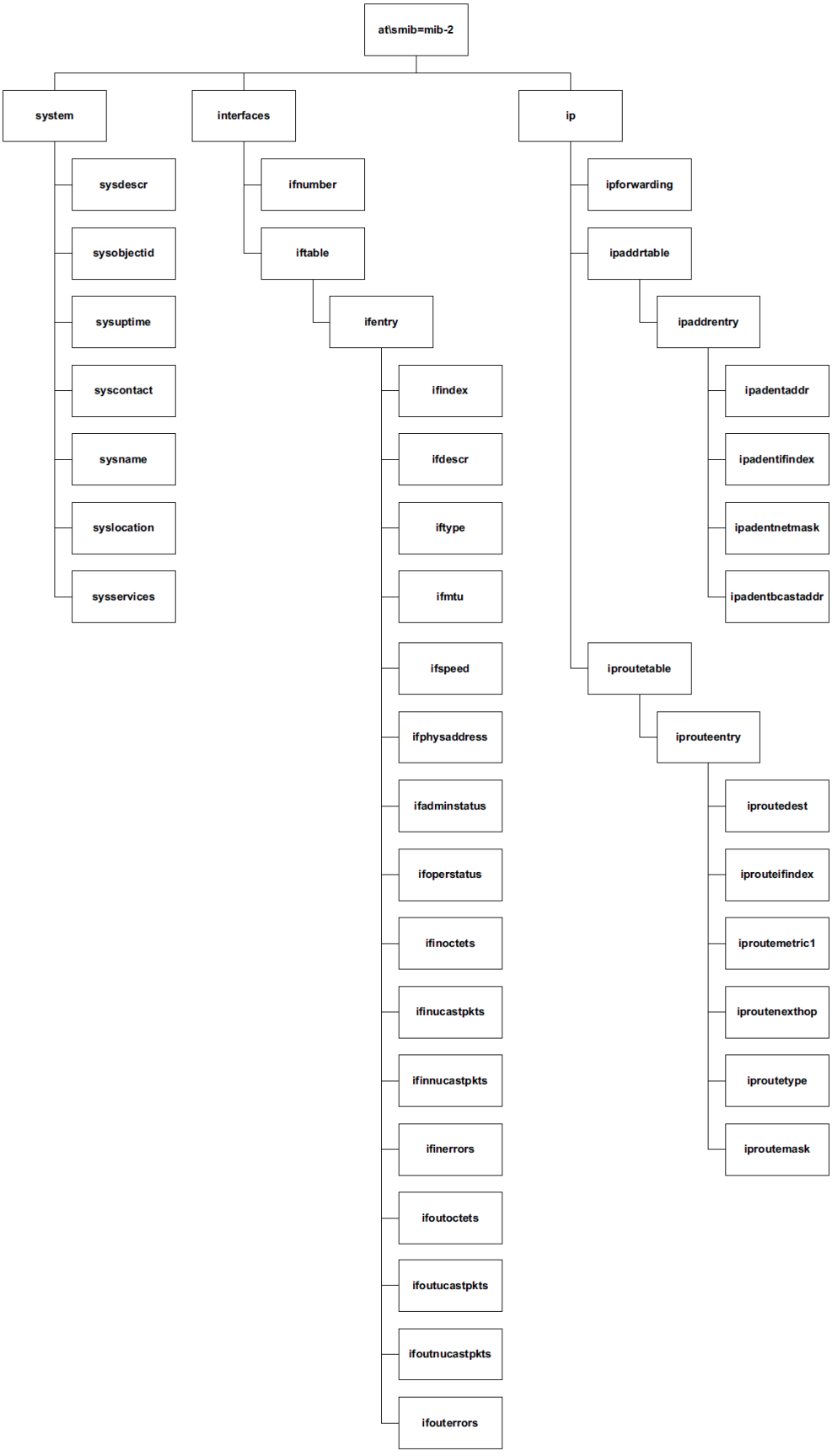
at\port?
PORT 2
ASY0
OK

Here, ASY2 is the active port and ASY0 is the port at which the command was entered. If the default port and the port to which you are connected are the same, only one entry will be listed.

To reset the default port to the one to which you are connected use the AT\PORT command without a parameter.

\smib Commands

The at\smib command allows you to view a single standard MIB variable. To view the variable use the at\smib=<mib_name> command, where <mib_name> is the variable to be displayed. The variables are sorted according to the hierarchy shown below.


at\smib=mib-2
system
interfaces
ip
sysdescr
sysobjectid
sysuptime
syscontact
sysname
syslocation
sysservices
ifnumber
iftable
ifentry
ifindex
ifdescr
iftype
ifmtu
ifspeed
ifphysaddress
ifadminstatus
ifoperstatus
ifinoctets
ifinucastpkts
ifinnucastpkts
ifinerrors
ifoutoctets
ifoutucastpkts
ifoutnucastpkts
ifouterrors
ipforwarding
ipaddrtable
ipaddrentry
ipadentaddr
ipadentifindex
ipadentnetmask
ipadentbcastaddr
iproutetable
iprouteentry
iproutedest
iprouteifindex
iproutemetric1
iproutenexthop
iproutetype
iproutemask

System

The System hierarchy consists of the following:

at\smib=mib-2.system.sysdescr

This variable shows the software version information (equivalent to what is shown on the 'ati5' CLI command output).

```
mib-2.system.sysdescr =
Software Build Ver5121.  Jan 31 2011 12:26:04  9W
```

at\smib=mib-2.system.sysobjectid

The authoritative identification of the network management subsystem. The Digi does not support outputting OID variables. Instead, "*oid*" is output.

```
mib-2.system.sysobjectid = oid
```

at\smib=mib-2.system.sysuptime

The time the unit has been running in 10msec units (hundredths of a second).

```
mib-2.system.sysuptime = 1806718
```

The above example shows that the unit has been running for 5 hours, 1 minute and 7.18 seconds.

at\smib=mib-2.system.syscontact

A description of the contact person for the unit. For the Digi, this is always a zero-length string.

at\smib=mib-2.system.sysname

The name of the unit (the name set in the **Router Identity** parameter on the ***Configuration - System > Device Identity*** page).

```
mib-2.system.sysname = digi.router
```

at\smib=mib-2.system.syslocation

The physical location of the unit. For the Digi, this is always a zero-length string.

at\smib=mib-2.system.sysservices

This variable displays a value that represents the set of services the unit provides. For each OSI layer the unit provides services for, 2(L-1) is added to the value, where L is the layer. The layers are shown below:

Layer	Functionality
1	Physical
2	Data Link
3	Network
4	Transport
5	Session
6	Presentation
7	Application

For the Digi, this value is always 7 (Physical layer (21-1) + Data Link layer (22-1) + Network layer (23-1)).

Interfaces

The Interfaces hierarchy consists of the ifnumber variable and the iftable node:

at\smib=mib-2.interfaces.ifnumber

The total number of interfaces on the unit. This includes Ethernet, PPP and virtual interfaces (i.e. IPSec tunnels) and SYNC ports.
`mib-2.interfaces.ifnumber = 52`

at\smib=mib-2.interfaces.iftable

The iftable node contains ifentry nodes for each interface. For each table entry, an index specifier must be appended to the end of each variable (e.g. for PPP0, 1 must be appended).

at\smib=mib-2.interfaces.iftable.ifentry

at\smib=mib-2.interfaces.iftable.ifentry.ifindex

The unique index number of the interface.

at\smib=mib-2.interfaces.iftable.ifentry.ifdescr

This variable displays information about the interface. This information is displayed in the format *<interface type>-<instance>*, where:

<interface type> can be one of *PPP*, *ETH*, *TUN* (for IPSec tunnels), *SNAIP* (for SNAIP links) or *SYNC*, and

<instance> is the instance.

For example:
`mib-2.interfaces.iftable.ifentry.ifdescr.1 = PPP-0`

at\smib=mib-2.interfaces.iftable.ifentry.iftype

The type of interface, as described by the physical/link protocol below the network layer in the protocol stack. Values can be one of the following:

PPP	23
ETH	6
IPSec Tunnel	131
SNAIP	17
SYNC port	118

For example:
`mib-2.interfaces.iftable.ifentry.iftype.1 = 23`

at\smib=mib-2.interfaces.iftable.ifentry.ifmtu

The size of the largest datagram (in octets) which can be sent on the interface. SNAIP and SYNC ports always return 0. IPSec tunnel interfaces will return the underlying interface if it can be located, otherwise 0 is returned. PPP interfaces will return the negotiated MTU if the link is connected, otherwise 0 is returned.

For example:
`mib-2.interfaces.iftable.ifentry.ifmtu.21 = 1504`

at\smib=mib-2.interfaces.iftable.ifentry.ifspeed

This variable displays an estimate of the interface's current bandwidth in bits per second. SNAIP and SYNC ports will always return 0. PPP ports will always return 64000.

For example:
`mib-2.interfaces.iftable.ifentry.ifspeed.1 = 64000`

at\smib=mib-2.interfaces.iftable.ifentry.ifphysaddress

The interface's address at the protocol layer immediately below the network layer in the protocol stack. For interfaces without such an address, a zero-length octet string is returned. For PPP, SNAIP and SYNC ports, a 0 length string is returned.

at\smib=mib-2.interfaces.iftable.ifentry.ifadminstatus

The desired state of the interface. The testing state (3) indicates no operational packets can be passed.

at\smib=mib-2.interfaces.iftable.ifentry.ifoperstatus

The current operational state of the interface. The testing state (3) indicates no operational packets can be passed.

at\smib=mib-2.interfaces.iftable.ifentry.ifinoctets

The total number of octets received on this interface, including framing characters.

at\smib=mib-2.interfaces.iftable.ifentry.ifinucastpkts

The number of subnetwork-unicast packets delivered by this interface to a higher-layer protocol.

at\smib=mib-2.interfaces.iftable.ifentry.ifinnucastpkts

The number of non-unicast (i.e. broadcast or multicast) packets delivered by this interface to a higher-layer protocol.

at\smib=mib-2.interfaces.iftable.ifentry.ifinerrors

The number of inbound packets received by this interface that contained errors preventing them from being delivered to a higher-level protocol.

at\smib=mib-2.interfaces.iftable.ifentry.ifoutoctets

The total number of octets transmitted by this interface, including framing characters.

at\smib=mib-2.interfaces.iftable.ifentry.ifoutucastpkts

The total number of packets that higher-level protocols requested this interface to transmit to a subnetwork-unicast address, including those that were discarded or not sent.

at\smib=mib-2.interfaces.iftable.ifentry.ifoutnucastpkts

The total number of packets that higher-level protocols requested this interface to transmit to a non-unicast (i.e. broadcast or multicast) address, including those that were discarded or not sent.

at\smib=mib-2.interfaces.iftable.ifentry.ifouterrors

The number of outbound packets that this interface could not transmit because of errors.

IP

The IP node consists of the ipforwarding variable and the ipaddrtable and iproutetable nodes.

at\smib=mib-2.ip.ipforwarding

This variable indicates whether the unit is acting as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to, the unit. IP gateways forward datagrams, IP hosts do not. For the Digi, this value is always 1.

at\smib=mib-2.ip.ipaddrtable

The ipaddrtable node contains ipaddrentry nodes for each IP address assigned to each interface of the unit. For each table entry, an index specifier must be appended to the end of each variable that specifies the interface (e.g. for PPP0, 1 must be appended).

at\smib=mib-2.ip.ipaddrtable.ipaddrentry

at\smib=mib-2.ip.ipaddrtable.ipaddrentry.ipadentaddr

The IP address to which this entry's addressing information pertains.

at\smib=mib-2.ip.ipaddrtable.ipaddrentry.ipadentifindex

The index identifier for the interface associated with this IP address.

at\smib=mib-2.ip.ipaddrtable.ipaddrentry.ipadentnetmask

The subnet mask associated with the IP address.

at\smib=mib-2.ip.ipaddrtable.ipaddrentry.ipadentbcastaddr

The value of the least-significant bit in the IP broadcast address used for sending datagrams on the IP address of this interface.

at\smib=mib-2.ip.iproutetable

The iproutetable node contains iprouteentry nodes for each route defined on the unit.

at\smib=mib-2.ip.iproutetable.iprouteentry

at\smib=mib-2.ip.iproutetable.iprouteentry.iproutedest

The destination IP address for the route. An entry with a value of 0.0.0.0 is considered the default route. Multiple routes to a single destination can appear in the routing table, but access to such multiple entries is dependant on the table-access mechanisms defined by the network management protocol in use.

at\smib=mib-2.ip.iproutetable.iprouteentry.iprouteifindex

The index value which uniquely identifies the local interface through which the next hop of the route should be reached.

at\smib=mib-2.ip.iproutetable.iprouteentry.iproutemetric1

The primary routing metric for the route.

at\smib=mib-2.ip.iproutetable.iprouteentry.iproutenexthop

The IP address of the next hop of the route.

at\smib=mib-2.ip.iproutetable.iprouteentry.iproutetype

The type of route. Valid values are:

1	Valid
2	Invalid
3	Direct
4	Indirect

at\smib=mib-2.ip.iproutetable.iprouteentry.iproutemask

The netmask for the route.

"S" REGISTERS

In addition to the AT commands there are a number of Special ("S") registers. These registers contain numeric values that may represent time intervals, ASCII characters or operational flags.

To display the contents of a particular "S" register, the ATS command is used in the form ATSn? where n is the number of the register whose contents are to be shown.

To store a new value into a register, use the S command in the form ATSN=X where N is the number of the register to be changed and X is the new value. For example, ATS31=4 would store the value 4 in S31.

The unit maintains one set of registers for each ASY port. By default, the S command operates ONLY on the S register set for the active port. To select an alternative default port, use the AT\PORT command first.

Each register can only be set to a limited range of values as shown in the table below:

Reg.	Description	Units	Default	Range
S0	V.120 Answer enable	Rings	0	0-255
S1	Ring count	Rings	n/a	n/a
S2	Escape character	ASCII	43	0-255
S9	DCD on delay	ms x 20	0	0-255
S10	Pulse time for DCD Low	ms x 10	0	0-255
S12	Escape delay	ms	50	0-255
S15	Data forwarding timer	ms	2	0-255
S23	Parity	N/A	0	0-2 5 6
S31	ASY interface speed	refer to full description	n/a	0-11
S33	DTR dialling	N/A	0	0 1
S45	DTR loss de-bounce	0.05 seconds	(0.25s)	1-255

S0 V.120 Answer Enabled

Units: Rings
Default: 0
Range: 0-255

S0 is used only in V.120 mode to enable or disable automatic answering of incoming ISDN calls. Auto answering is disabled when S0 is set to the default value of 0. Setting S0 to a non-zero value enables auto-answering.

The actual value stored determines the number of "rings" that the unit will wait before answering. For example, the command ATS0=2 enables auto-answering after two incoming rings have been detected.

With each ring the RING result code is issued and the value stored in S1 is incremented. When the value in S1 equals the value in S0 the call is answered.

S1 Ring count

Units: Rings
Default: n/a
Range: n/a

When ADAPT detects an incoming ISDN call on an ASY port, it will print “RING” to the ASY port at 2 second intervals. It also increments the S1 register, counting how many times “RING” is printed.

S2 Escape Character

Units: ASCII
Default: 43
Range: 0-255

The value stored in S2 defines which ASCII character is used as the Escape character, which by default is the “+” symbol. Entering this character three times followed by a delay of 1-2 seconds and then an AT command will cause the unit to switch from on-line mode to command mode.

S12 Escape Delay

Units: ms
Default: 50
Range: 0-255

The value stored in S12 defines the delay between sending the escape sequence and entering an AT command for the unit to switch from on-line mode to command mode.

S15 Data Forwarding Timer

Units: 10ms
Default: 0
Range: 0-255

S15 is used to set the data forwarding timer for the ASY port in multiples of 10ms. The default data forwarding time is 20ms and in normal use this there should be no need to change this. However, setting S15 to 1 enables a special mode of operation in which data is forwarded as fast as possible for the data rate for which the port is configured (at 115000bps this will typically be 2-3ms).

Note that the default value of 0 is equivalent to setting the register to 2 in order to maintain compatibility with older systems.

S23 Parity

Units: N/A
Default: 0
Range: 0-2,5,6

The value stored in S23 determines whether the parity used for the ASY port is set to None (0), Odd (1), Even (2), 8Data Odd (5) or 8Data Even (6).

S31 ASY Interface Speed

Units: N/A
Default: 0
Range: 0-11

Register S31 is used to set the speed and data format for the ASY port to which you are currently connected.

The default value for ASY 0 is 0, i.e. the port speed/data format is not set to a specific value, it is determined automatically from the AT commands that you enter.

The default value for ASY 1, 2 and 3 is 3, i.e. the ports will only accept AT commands at 115,200bps (8 data bits, no parity and 1 stop bit).

To set the speed of one of the ports to a particular value, the appropriate register should be set to the required value from the following table:

S31	Port Speed (bps)	S31	Port Speed (bps)
0	Auto-detect	6	19200
1	Reserved	7	9600
2	Reserved	8	4800
3	115200	9	2400
4	57600	10	1200
5	38400	11	300

For example, to change the speed of ASY 1 to 38,400bps, connect your terminal to that port with the speed set to 9600bps. Enter the command:

ats31=5

then change the speed of your terminal to 38,400bps before entering any more AT commands.

The data format used when the ATS31=n command is entered is selected as the data format for all further commands.

The auto-detect option is only available for ASY0 and ASY1.

S33 DTR Dialling

Units: N/A
Default: 0
Range: 0, 1

S33 is used to enable or disable DTR dialling for the port. When DTR dialling is enabled, the unit will dial the number stored for that port (see AT&Z) when the DTR signal from the terminal changes from Off to On.

S45 DTR Loss De-Bounce

Units: 0.05 seconds
Default: 5
Range: 1-255

The value in S45 determines the length of time for which the DTR signal from the terminal device must go off before the unit acts upon any options that are set to trigger on loss of DTR. Increasing or decreasing the value in S45 makes the unit less or more sensitive to “bouncing” of the DTR signal respectively.

GENERAL SYSTEM COMMANDS

The application commands described in this section are basic configuration commands that do not relate to specific types of application or network.

CONFIG Show / Save Configuration

The config command is used for the following purposes to show current or stored configuration settings, to save the current configuration or to specify which configuration is to be used when the unit is powered up or rebooted.

The format of the config command is:

config <0|1|c> <save|show|powerup>

Two separate configurations can be stored, numbered 0 and 1. The first parameter of the config command specifies to which configuration the command applies. The letter “c” denotes the current configuration settings, i.e. those currently in use.

The second parameter is one of the following keywords:

show displays the specified configuration (either 0, 1 or c for the current configuration)

save saves the current settings as the specified configuration (either 0 or 1)

powerup sets the specified configuration (either 0 or 1) to be used at power-up or reboot

For example, to display the current configuration use the command:

config c show

The output will appear similar to the following example:

```
config c show
eth 0 descr "LAN 0"
eth 0 IPaddr "192.168.1.1"
eth 0 mask "255.255.255.0"
eth 0 bridge ON
eth 1 descr "LAN 1"
eth 2 descr "LAN 2"
eth 3 descr "LAN 3"
eth 4 descr "ATM PVC 0"
```

The config files only contain details of those settings that are different from the unit’s default settings. If you make a setting that is the same as the default setting, it will not appear in a stored configuration.

To save the current settings to configuration file 1, enter:

config 1 save

To use configuration 1 when the unit is powered up or rebooted, enter:

config 1 powerup

Config changes counter

The config changes command shows the number of changes to the current configuration since the unit has powered up and the initial configuration file run. Also shows the time when the config file was last saved.

REBOOT Reboot Unit

The ***reboot*** command causes the unit to execute a complete hardware reset, loading and running the main image file from cold. It has three modes of operation:

reboot - will reboot the unit after any FLASH write operations have been completed. Also, 1 second each is allowed for the following operations to be completed before reboot will take place:

- IPSec SA delete notifications have been created and sent
- TCP sockets have been closed
- PPP interfaces have been disconnected

reboot <n> - will reboot the unit in <n>minutes where n is 1 to 65,535

reboot cancel - will cancel a timed reboot if entered before the time period has passed.

Reset router to factory defaults

See reference guide section titled “Administration - Factory Default Settings”.

Disabling the reset button

Normally when the reset button is held in for 5 seconds the router is reset to factory defaults. The factory reset button functionality can be disabled / enabled if required.

The command to disable the reset button is “*cmd 0 pbreset off*”

To re-enable the reset button functionality “*cmd 0 pbreset on*”

TEMPLOG Temperature monitoring

The on-board temperature sensors are sampled every 60 seconds and any 'interesting' changes in the temperature are logged to a special flash file, 'templog.c1'. Use '*templog 0 status*' to view the last stored record in this file.

There are 2 sensors built in, there is one on the motherboard and one on the modem module. If a temperature is reached that is outside of normal operating limits, an event will be logged in the eventlog.txt
Note: The only transport models that support TEMPLOG are DR64 and VC7400.

Ping and Traceroute

From the CLI, these commands can be used to help troubleshoot connectivity problems.

The syntax of the ping command is:

ping <ip address|FQDN> [n]

Where n (if used) is the number of ICMP echo requests to send. If not specified, only 1 echo request will be sent.

To stop pings when n has been set to a high value use *ping stop*

The syntax of the traceroute command is:

traceroute <ip address|FQDN>

To stop a failed trace if hosts can not be detected, use *traceroute stop*

Clearing the Analyser Trace and Event Log

To clear the analyser trace, the CLI command is *ana 0 anaclr*

To clear the event log, the CLI command is *clear_ev*

Activate and Deactivate interfaces

To manually activate (or raise) an interface, the following CLI command can be used as an activation request.

<entity> <instance> act_rq

To manually deactivate (or lower) an interface, the following CLI command can be used as an activation request.

<entity> <instance> deact_rq

Where *<entity>* can be:

PPP for PPP interfaces
TUN for GRE TUN interfaces
OVPN for OpenVPN interfaces

And *<instance>* is the interface number, such as 0, 1, 2 etc

For example, to activate PPP 1, the CLI command would be:

ppp 1 act_rq

and to deactivate PPP 1:

ppp 1 deact_rq

Special Usernames

There are some special usernames that can also be used for both local and remote authentication, these are:

%s This uses the serial number of the router as the username.

%i This uses the IMEI of the cellular module as the username.

%c This uses the ICCID of the SIM as the username.

If a '%' symbol is part of the username, it must be escaped with another '%' symbol. For example, 'user%1' should be entered as 'user%%1'.

GPIO (General Purpose Input Output)

GPIO commands are necessary to configure a WR44, which has one Digital Input/Output port and one Digital Input port. This command allows configuration of the I/O port either as an input port or an output port. For example:

Command	Description
gpio inout input	Configures the I/O port as an input.
gpio inout output	Configures the I/O port as an output.
gpio inout ON	Sets the I/O port to ON when configured as an output.
gpio inout OFF	Sets the I/O port to OFF when configured as an output.

The syntax of the command is as follows:

Usage: *gpio [inout ON|OFF|input|output]*

With no parameters, the command will display the current status of the ports. For example:

```
gpio
Input(s):
         in : OFF
Output(s):
      inout : OFF
OK
```

To set the I/O port to be an output:

```
gpio inout output
Input(s):
         in : OFF
Output(s):
      inout : OFF
OK
```

To set the I/O port to ON when it is configured as an output:

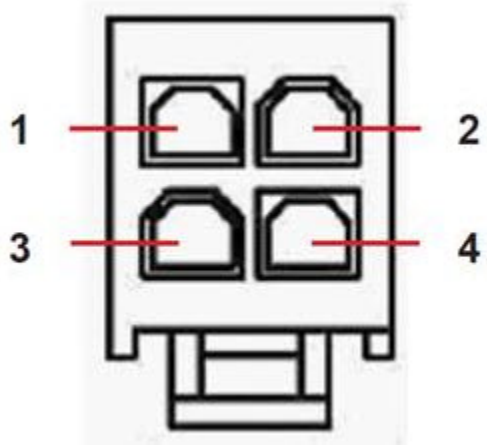
```
gpio inout on
Input(s):
         in : OFF
Output(s):
      inout : ON
OK
```

The Input and Input/Output connections (pins 2 and 3) are programmed via the command line using the gpio command. The default setting for pins 2 and 3 are OFF as seen in the above example.

Note:
Only one of the power connectors should be used. Never apply power to both the MAIN and AUX connectors at the same time.

Pin	Description
Pin 1	GROUND
Pin 2	INPUT
Pin 3	Input/ Output
Pin 4	Power

The following image shows the pins and the corresponding numbers:



For more information on wiring and other details, refer to *Digi Transport 4-pin DC Power Cord User Guide*.

GOBI Image Load Selection

For the qdl command, it is used to specify which image to load onto a GOBI cellular module.

The syntax of the command is:

```
qdl 0 fw <n>
```

where n can be 0 .. 14. The default value is 0.

Instance	Value
0	Generic UMTS
1	Verizon
2	Sprint PCS
3	IUSACELL
4	Bell Mobility
5	Alltel
6	Cingular Blue
7	Cingular Orange
8	T-Mobile
9	Docomo
10	Orange
11	Vodafone
12	Telefonica
13	Telital
14	OMH

TCPPERM AND TCPDIAL

This section describes the operation of the tcpperm and tcpdial commands which are available only as application commands and have no equivalent web pages.

TCPPERM

The tcpperm command is used to establish a permanent "serial to IP" connection between one of the ASY ports and a remote IP host. After the command has been executed, the unit will automatically open a socket connection to the remote peer whenever data is received from a terminal attached to the specified ASY port. When the socket is first opened and the connection has been established, the unit will issue a CONNECT message to the terminal and will subsequently relay data between the socket and the ASY port. The format of the CONNECT message can be modified using the standard AT commands (e.g. ATV, ATE, etc.) or using the Configuration - Network > Interfaces > Serial > Serial Port n web page.

Note:
The serial port should also be pre-configured to use the appropriate word format, speed and flow control.

While the serial-to-IP connection is established, if the attached serial device drops the DTR signal, then the socket connection will be terminated, much as with a standard modem or terminal adapter. Again this behaviour can be modified via the AT&D command or the serial port settings.

The format of the command is:

```
TCPPERM <[ASY 0-1]> <Dest Host> <Dest Port> [UDP] [nodeact] [-
l<listening port>] [-i<inact_timeout>] [-f<fwd_time>] [-e<eth_ip>][-
d(deact link)] [-k<keepalive_time>] [-s<src_port>] [-ok] [-
t<telnet_mode>] [-ho(host only)] [-ssl] [-ao(always open)] [-m<mhome
idx>]
```

The parameters are detailed in the following table:

Parameter	Description
ASY	The number of the ASY port that the link will be made from/to
Dest Host	The IP address (or name) of the remote peer
Dest Port	The port number to use on the remote peer
UDP	Open a UDP connection (the default is TCP)
-ao	Open socket immediately, and reopen if and when the socket is closed
-e	Use the address of ethernet port 'n' for the socket connection rather than the default of the address of the interface over which the socket is opened (i.e ppp 1, ppp 2, etc.)
-d	Deactivate link - if non-zero, when the socket is closed and there are no other sockets using the interface then the interface connection is dropped (switched connections only)
-f	The forwarding time (x10ms) for packetising data from the serial port
-ho	Host - indicates that the socket should only accept connections from the specified host.

Parameter	Description
-i	The inactivity timeout (s) after which the socket will be closed
-k	Keep alive packet timer (s)
-l	Listening port - allows the user to set a new TCP port number to listen on rather than the default value of 4000+ASY port #
-m	Multihome additional consecutive addresses index
-ok	Open socket in 'quiet mode', i.e. there is no 'OK' response to the TCPPERM command.
-s	Source port number
-ssl	Use SSL mode
-t	Use Telnet mode. Opens socket in the corresponding Telnet mode (port 23 default), 0= raw, 1 Telnet Mode, 2 - Telnet Mode with null stuffing. If this is not specified then the mode specified for the associated ASY port in general setup is used. If the -t option is specified then the "ok" option is always used.

The command can also be made to execute automatically on power-up by using the "cmd n autocmd 'cmd'" macro command, i.e.

cmd 0 autocmd 'tcpperm asy 0 192.168.0.1 -f3 -s3000 -k10 -e1'

Considerations for use with VPN or GRE Tunnels

When the socket used by TCPPERM is opened the default behaviour is to use the address of the interface over which the socket is carried (ETHn or PPPn) as the source address of the socket. If the socket data is to be tunnelled then it may be necessary to use the -en modifier so that the source address of the socket matches the local subnet address specified in the appropriate Eroute. A similar effect can also be achieved by setting the parameter Default source IP address interface: Ethernet n in the Web interface on the Configuration - Network > Advanced Network Settings.

TCPDIAL

TCPDIAL operates in an identical manner to TCPPERM except that establishment of the socket connection is not automatic and must be initiated by the tcpdial command. The simplest method of achieving this is to map a command using the ***Configuration - Network > Interfaces > Serial > Command Mappings***, i.e. Command to Map ATDT0800456789 maps to "tcpdial asy 1 217.36.133.29 -e0". Now, whenever the attached terminal device attempts to dial the number defined the unit will map it to an IP socket connection.

In this way multiple dial commands can be directed to the same or different IP hosts with other simple command mappings.

Aborting TCPDIAL

The tcpdab command can be used to cancel a TCPDIAL connection before the connection has been made. It can also be used from a command session to disconnect an existing TCPDIAL connection on another ASY port.

The format of the command is:

tcpdab <instance> ATH

where <*instance*> is the number of the ASY port.

SERIAL PORT CONNECTIONS

Depending upon the model, the asynchronous serial ports on may be presented as DB 25 sockets, DB 9 sockets or 8-pin RJ45 sockets. On some models, a combination of the above may be used. The following tables list the pin designations of each type of connector for each Digi model.

The RS-232 port pin-outs are suitable for both Async and Sync port connections. When used in Async mode the pins for TxC, RxC & ETC are not required, these are needed for Sync mode only.

RS-232 Port Pin-Outs

			DB 25	RJ45
				
Description	**RS232 signal**	**Direction**[1]	**Pin #**	**Pin #**
Transmit Data	TxD	**in**	2	6
Receive Data	RxD	**out**	3	3
Ready To Send	RTS	**in**	4	1
Clear To Send	CTS	**out**	5	8
Data Set Ready	DSR	**out**	6	n/a
Ground	GND	**n/a**	7	5
Data Carrier Detect	DCD	**out**	8	7
Transmitter Clock	TxC	**out**	15	n/a
Receiver Clock	RxC	**out**	17	n/a
Data Terminal Ready	DTR	**in**	20	2
Ring Indicate	RI	**out**	22	n/a
External Transmitter Clock	ETC	**in**	24	n/a

1. With respect to Digi units

X.21 (RS-422)

Note:
In order for the DR64x0(W) to operate in X.21 mode, a kepler daughter card must be fitted.

			DB 25
			
Description	**X.21 signal**	**Direction**[1]	**Pin #**
Receive Data (A)	RxDA	**out**	3
Receive Data (B)	RxDB	**out**	16
Transmit Data (A)	TxDA	**in**	2
Transmit Data (B)	TxDB	**in**	14
Indication (B)	INDB	**out**	13
Ground	GND	**n/a**	7
Control (B)	CTLB	**in**	19
Clock (A)	CLKA	**in or out**[2]	17
Clock (B)	CLKB	**in or out**[2]	9
Indication (A)	INDA	**out**	5
Control (A)	CTLA	**in**	4

1. With respect to Digi units
2. Direction depends on whether the Digi unit is clock sink or clock source.

X.21 25-Pin to 15-Pin Straight Through Cable – Internal Clock

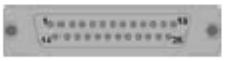
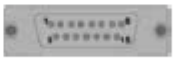
This is normally the cable to use to connect an X.21 terminal (e.g. an ATM) to the Digi. Use this cable when the Digi is the clock ***source*** or configured as "internal clock".

DB 25- Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
RxDA	3	4	RxDA
RxDB	16	11	RxDB
TxDA	2	2	TxDA
TxDB	14	9	TxDB
INDB	13	12	INDB
GND	7	8	GND
CTLB	19	10	CTLB
CLKB	9	13	CLKB
CLKA	17	6	CLKA
INDA	5	5	INDA
CTLA	4	3	CTLA

N.B. Frame Ground is optional.

X.21 25-Pin to 15-Pin Straight Through Cable – External Clock

This is normally the cable to use to connect an X.21 terminal (e.g. an ATM) to the Digi. Use this cable when the Digi is the clock ***sink*** or configured as "external clock".

DB 25- Digi Side		DB 25	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
RxDA	3	4	RxDA
RxDB	16	11	RxDB
TxDA	2	2	TxDA
TxDB	14	9	TxDB
INDB	13	12	INDB
GND	7	8	GND
CTLB	19	10	CTLB
CLKB	9	13	CLKB
CLKA	17	6	CLKA
INDA	5	5	INDA
CTLA	4	3	CTLA

N.B. Frame Ground is optional.

Note:

When operating an X.21 (RS-422) link Synchronously it is necessary to fit termination resistors to each signal pair at the receiving end. The Digi already has in-built terminating resistors, but terminating resistors will need to be fitted between the RxDA & RxDB pins, CLKA & CLKB pins and INDA & INDB pins at the DTE.

X.21 25-Pin to 15-Pin Crossover Cable – Internal Clock

This is normally the cable to use to connect the Digi to an X.21 leased line. Use this cable when the Digi is the clock *source* or configured as "internal clock".

DB 25- Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
RxDA	3	2	TxDA
RxDB	16	9	TxDB
TxDA	2	4	RxDA
TxDB	14	11	RxDB
INDB	13	10	CTLB
GND	7	8	GND
CTLB	19	12	INDB
CLKB	9	13	CLKB
CLKA	17	6	CLKA
INDA	5	3	CTLA
CTLA	4	5	INDA

N.B. Frame Ground is optional.

X.21 25-Pin to 15-Pin Crossover Cable – External Clock

This is normally the cable to use to connect the Digi to an X.21 leased line. Use this cable when the Digi is the clock *sink* or configured as "external clock".

DB 25- Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	1	1	Frame Ground (Case)
RxDA	3	2	TxDA
RxDB	16	9	TxDB
TxDA	2	4	RxDA
TxDB	14	11	RxDB
INDB	13	10	CTLB
GND	7	8	GND
CTLB	19	12	INDB
CLKB	9	13	CLKB
CLKA	17	6	CLKA
INDA	5	3	CTLA
CTLA	4	5	INDA

N.B. Frame Ground is optional.

Note:

When operating an X.21 (RS-422) link Synchronously it is necessary to fit termination resistors to each signal pair at the receiving end. The Digi already has in-built terminating resistors, but terminating resistors will need to be fitted between the TxDA & TxDB pins, CLKA & CLKB pins and CTLA & CTLB pins at the DTE.

WR44

RS-232 Port Pin-Outs

			DB 25	DB 9	RJ45
					
Description	**RS232 signal**	**Direction[1]**	**Pin #**	**Pin #**	**Pin #**
Transmit Data	TxD	**in**	2	3	6
Receive Data	RxD	**out**	3	2	3
Ready To Send	RTS	**in**	4	7	1
Clear To Send	CTS	**out**	5	8	8
Data Set Ready	DSR	**out**	6	6	n/a
Ground	GND	**n/a**	7	5	5
Data Carrier Detect	DCD	**out**	8	1	7
Transmitter Clock	TxC	**out**	15	n/a	n/a
Receiver Clock	RxC	**out**	17	n/a	n/a
Data Terminal Ready	DTR	**in**	20	4	2
Ring Indicate	RI	**out**	22	9	n/a
External Transmitter Clock	ETC	**in**	24	n/a	n/a

1. With respect to Digi units

X.21 (RS-422)

Note:
In order for the WR44 to operate in X.21 mode, a Viper daughter card must be fitted.

			DB 25
			
Description	**X.21 signal**	**Direction[1]**	**Pin #**
Transmit Data (A)	TxDA	**in**	2
Receive Data (A)	RxDA	**out**	3
Control (A)	CTLA	**in**	4
Indication (A)	INDA	**out**	5
Ground	GND	**n/a**	7
Clock (B)	CLKB	**in or out[2]**	9
Indication (B)	INDB	**out**	13
Transmit Data (B)	TxDB	**in**	14
Receive Data (B)	RxDB	**out**	16
Clock (A)	CLKA	**in or out[2]**	17
Control (B)	CTLB	**in**	19

1. With respect to Digi units
2. Direction depends on whether the Digi unit is clock sink or clock source.

X.21 25-Pin to 15-Pin Straight Through Cable – Internal Clock

This is normally the cable to use to connect an X.21 terminal (e.g. an ATM) to the Digi. Use this cable when the Digi is the clock *source* or configured as "internal clock".

DB 25- Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
RxDA	3	4	RxDA
RxDB	16	11	RxDB
TxDA	2	2	TxDA
TxDB	14	9	TxDB
INDB	13	12	INDB
GND	7	8	GND
CTLB	19	10	CTLB
CLKB	9	13	CLKB
CLKA	17	6	CLKA
INDA	5	5	INDA
CTLA	4	3	CTLA

N.B. Frame Ground is optional.

X.21 25-Pin to 15-Pin Straight Through Cable – External Clock

This is normally the cable to use to connect an X.21 terminal (e.g. an ATM) to the Digi. Use this cable when the Digi is the clock *sink* or configured as "external clock".

DB 25- Digi Side		DB 25	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
RxDA	3	4	RxDA
RxDB	16	11	RxDB
TxDA	2	2	TxDA
TxDB	14	9	TxDB
INDB	13	12	INDB
GND	7	8	GND
CTLB	19	10	CTLB
CLKB	9	13	CLKB
CLKA	17	6	CLKA
INDA	5	5	INDA
CTLA	4	3	CTLA

N.B. Frame Ground is optional.

Note:

When operating an X.21 (RS-422) link Synchronously it is necessary to fit termination resistors to each signal pair at the receiving end. The Digi already has in-built terminating resistors, but terminating resistors will need to be fitted between the RxDA & RxDB pins, CLKA & CLKB pins and INDA & INDB pins at the DTE.

X.21 25-Pin to 15-Pin Crossover Cable – Internal Clock

This is normally the cable to use to connect the Digi to an X.21 leased line. Use this cable when the Digi is the clock ***source*** or configured as "internal clock".

DB 25- Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
RxDA	3	2	TxDA
RxDB	16	9	TxDB
TxDA	2	4	RxDA
TxDB	14	11	RxDB
INDB	13	10	CTLB
GND	7	8	GND
CTLB	19	12	INDB
CLKB	9	13	CLKB
CLKA	17	6	CLKA
INDA	5	3	CTLA
CTLA	4	5	INDA

N.B. Frame Ground is optional.

X.21 25-Pin to 15-Pin Crossover Cable – External Clock

This is normally the cable to use to connect the Digi to an X.21 leased line. Use this cable when the Digi is the clock ***sink*** or configured as "external clock".

DB 25- Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	1	1	Frame Ground (Case)
RxDA	3	2	TxDA
RxDB	16	9	TxDB
TxDA	2	4	RxDA
TxDB	14	11	RxDB
INDB	13	10	CTLB
GND	7	8	GND
CTLB	19	12	INDB
CLKB	9	13	CLKB
CLKA	17	6	CLKA
INDA	5	3	CTLA
CTLA	4	5	INDA

N.B. Frame Ground is optional.

Note:

When operating an X.21 (RS-422) link Synchronously it is necessary to fit termination resistors to each signal pair at the receiving end. The Digi already has in-built terminating resistors, but terminating resistors will need to be fitted between the TxDA & TxDB pins, CLKA & CLKB pins and CTLA & CTLB pins at the DTE.

RS-232 Port Pin-Outs

			DB 25	DB 9
				
Description	**RS232 signal**	**Direction**[1]	**Pin #**	**Pin #**
Transmit Data	TxD	**in**	2	3
Receive Data	RxD	**out**	3	2
Ready To Send	RTS	**in**	4	7
Clear To Send	CTS	**out**	5	8
Data Set Ready	DSR	**out**	6	6
Ground	GND	**n/a**	7	5
Data Carrier Detect	DCD	**out**	8	1
Transmitter Clock	TxC	**out**	15	n/a
Receiver Clock	RxC	**out**	17	n/a
Data Terminal Ready	DTR	**in**	20	4
Ring Indicate	RI	**out**	22	9
External Transmitter Clock	ETC	**in**	24	n/a

1. With respect to Digi units

ER2110, IR2110 & MR2110

RS-232 Port Pin-Outs

			DB 25
			
Description	**RS232 signal**	**Direction**[1]	**Pin #**
Transmit Data	TxD	**in**	2
Receive Data	RxD	**out**	3
Ready To Send	RTS	**in**	4
Clear To Send	CTS	**out**	5
Data Set Ready	DSR	**out**	6
Ground	GND	**n/a**	7
Data Carrier Detect	DCD	**out**	8
Transmitter Clock	TxC	**out**	15
Receiver Clock	RxC	**out**	17
Data Terminal Ready	DTR	**in**	20
Ring Indicate	RI	**out**	22
External Transmitter Clock	ETC	**in**	24

1. With respect to Digi units

RS-232 Port Pin-Outs

			DB
			
Description	**RS232 signal**	**Direction**[1]	**Pin #**
Transmit Data	TxD	**in**	2
Receive Data	RxD	**out**	3
Ready To Send	RTS	**in**	4
Clear To Send	CTS	**out**	5
Data Set Ready	DSR	**out**	6
Ground	GND	**n/a**	7
Data Carrier Detect	DCD	**out**	8
Transmitter Clock	TxC	**out**	15
Receiver Clock	RxC	**out**	17
Data Terminal Ready	DTR	**in**	20
Ring Indicate	RI	**out**	22
External Transmitter Clock	ETC	**in**	24

1. With respect to Digi units

GR2130

Port Pin-Outs

RS-232

			DB 25	RJ45
				
Description	**RS232 signal**	**Direction[1]**	**Pin #**	**Pin #**
Transmit Data	TxD	**in**	2	6
Receive Data	RxD	**out**	3	3
Ready To Send	RTS	**in**	4	1
Clear To Send	CTS	**out**	5	8
Data Set Ready	DSR	**out**	6	4
Ground	GND	**n/a**	7	5
Data Carrier Detect	DCD	**out**	8	7
Transmitter Clock	TxC	**out**	15	n/a
Receiver Clock	RxC	**out**	17	n/a
Data Terminal Ready	DTR	**in**	20	2
Ring Indicate	RI	**out**	22	n/a
External Transmitter Clock	ETC	**in**	24	n/a

1. With respect to Digi units

X.21 (RS-422)

Note:

In order for the GR2130 to operate in X.21 mode, an X.21 daughter card must be fitted, with the jumpers set correctly. See "Configuring X.21 on Older Models" on page 522.

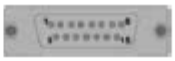
			DB 25
			
Description	**X.21 signal**	**Direction[1]**	**Pin #**
Receive Data (A)	RxDA	**out**	2
Receive Data (B)	RxDB	**out**	3
Transmit Data (A)	TxDA	**in**	4
Transmit Data (B)	TxDB	**in**	5
Indication (B)	INDB	**out**	6
Ground	GND	**n/a**	7
Control (B)	CTLB	**in**	8
Clock (B)	CLKB	**in or out[2]**	15
Clock (A)	CLKA	**in or out[2]**	17
Indication (A)	INDA	**out**	20
Control (A)	CTLA	**in**	22

1. With respect to Digi units

2. Direction depends on whether the Digi unit is clock sink or clock source.

X.21 25-Pin to 15-Pin Straight Through Cable – Internal Clock

This is normally the cable to use to connect an X.21 terminal (e.g. an ATM) to the Digi. Use this cable when the Digi is the clock *source* or configured as "internal clock".

DB 25- Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
RxDA	2	4	RxDA
RxDB	3	11	RxDB
TxDA	4	2	TxDA
TxDB	5	9	TxDB
INDB	6	12	INDB
GND	7	8	GND
CTLB	8	10	CTLB
CLKB	15	13	CLKB
CLKA	17	6	CLKA
INDA	20	5	INDA
CTLA	22	3	CTLA

N.B. Frame Ground is optional.

X.21 25-Pin to 15-Pin Straight Through Cable – External Clock

This is normally the cable to use to connect an X.21 terminal (e.g. an ATM) to the Digi. Use this cable when the Digi is the clock *sink* or configured as "external clock".

DB 25- Digi Side		DB 25	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
RxDA	2	4	RxDA
RxDB	3	11	RxDB
TxDA	4	2	TxDA
TxDB	5	9	TxDB
INDB	6	12	INDB
GND	7	8	GND
CTLB	8	10	CTLB
CLKB	15	13	CLKB
CLKA	17	6	CLKA
INDA	20	5	INDA
CTLA	22	3	CTLA

N.B. Frame Ground is optional.

Note:

When operating an X.21 (RS-422) link Synchronously it is necessary to fit termination resistors to each signal pair at the receiving end. The Digi already has in-built terminating resistors, but terminating resistors will need to be fitted between the RxDA & RxDB pins, CLKA & CLKB pins and INDA & INDB pins at the DTE.

X.21 25-Pin to 15-Pin Crossover Cable – Internal Clock

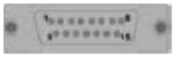
This is normally the cable to use to connect the Digi to an X.21 leased line. Use this cable when the Digi is the clock ***source*** or configured as "internal clock".

DB 25- Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
RxDA	2	2	TxDA
RxDB	3	9	TxDB
TxDA	4	4	RxDA
TxDB	5	11	RxDB
INDB	6	10	CTLB
GND	7	8	GND
CTLB	8	12	INDB
CLKB	15	13	CLKB
CLKA	17	6	CLKA
INDA	20	3	CTLA
CTLA	22	5	INDA

N.B. Frame Ground is optional.

X.21 25-Pin to 15-Pin Crossover Cable – External Clock

This is normally the cable to use to connect the Digi to an X.21 leased line. Use this cable when the Digi is the clock ***sink*** or configured as "external clock".

DB 25- Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	1	1	Frame Ground (Case)
RxDA	2	2	TxDA
RxDB	3	9	TxDB
TxDA	4	4	RxDA
TxDB	5	11	RxDB
INDB	6	10	CTLB
GND	7	8	GND
CTLB	8	12	INDB
CLKB	15	13	CLKB
CLKA	17	6	CLKA
INDA	20	3	CTLA
CTLA	22	5	INDA

N.B. Frame Ground is optional.

Note:

When operating an X.21 (RS-422) link Synchronously it is necessary to fit termination resistors to each signal pair at the receiving end. The Digi already has in-built terminating resistors, but terminating resistors will need to be fitted between the TxDA & TxDB pins, CLKA & CLKB pins and CTLA & CTLB pins at the DTE.

Port Pin-Outs

RS-232

			DB 25	RJ45
				
Description	**RS232 signal**	Direction[1]	Pin #	Pin #
Transmit Data	TxD	**in**	2	6
Receive Data	RxD	**out**	3	3
Ready To Send	RTS	**in**	4	1
Clear To Send	CTS	**out**	5	8
Data Set Ready	DSR	**out**	6	4
Ground	GND	**n/a**	7	5
Data Carrier Detect	DCD	**out**	8	7
Transmitter Clock	TxC	**out**	15	n/a
Receiver Clock	RxC	**out**	17	n/a
Data Terminal Ready	DTR	**in**	20	2
Ring Indicate	RI	**out**	22	n/a
External Transmitter Clock	ETC	**in**	24	n/a

1. With respect to Digi units

X.21 (RS-422)

Note:

In order for the IR2140 to operate in X.21 mode, an X.21 daughter card must be fitted, with the jumpers set correctly. See "Configuring X.21 on Older Models" on page 522.

			DB 25
			
Description	**X.21 signal**	Direction[1]	Pin #
Receive Data (A)	RxDA	**out**	2
Receive Data (B)	RxDB	**out**	3
Transmit Data (A)	TxDA	**in**	4
Transmit Data (B)	TxDB	**in**	5
Indication (B)	INDB	**out**	6
Ground	GND	**n/a**	7
Control (B)	CTLB	**in**	8
Clock (B)	CLKB	**in or out**[2]	15
Clock (A)	CLKA	**in or out**[2]	17
Indication (A)	INDA	**out**	20
Control (A)	CTLA	**in**	22

1. With respect to Digi units

2. Direction depends on whether the Digi unit is clock sink or clock source.

X.21 25-Pin to 15-Pin Straight Through Cable – Internal Clock

This is normally the cable to use to connect an X.21 terminal (e.g. an ATM) to the Digi. Use this cable when the Digi is the clock ***source*** or configured as "internal clock".

DB 25 - Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
RxDA	2	4	RxDA
RxDB	3	11	RxDB
TxDA	4	2	TxDA
TxDB	5	9	TxDB
INDB	6	12	INDB
GND	7	8	GND
CTLB	8	10	CTLB
CLKB	15	13	CLKB
CLKA	17	6	CLKA
INDA	20	5	INDA
CTLA	22	3	CTLA

N.B. Frame Ground is optional.

X.21 25-Pin to 15-Pin Straight Through Cable – External Clock

This is normally the cable to use to connect an X.21 terminal (e.g. an ATM) to the Digi. Use this cable when the Digi is the clock ***sink*** or configured as "external clock".

DB 25 - Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
RxDA	2	4	RxDA
RxDB	3	11	RxDB
TxDA	4	2	TxDA
TxDB	5	9	TxDB
INDB	6	12	INDB
GND	7	8	GND
CTLB	8	10	CTLB
CLKB	15	13	CLKB
CLKA	17	6	CLKA
INDA	20	5	INDA
CTLA	22	3	CTLA

N.B. Frame Ground is optional.

Note:

When operating an X.21 (RS-422) link Synchronously it is necessary to fit termination resistors to each signal pair at the receiving end. The Digi already has in-built terminating resistors, but terminating resistors will need to be fitted between the RxDA & RxDB pins, CLKA & CLKB pins and INDA & INDB pins at the DTE.

X.21 25-Pin to 15-Pin Crossover Cable – Internal Clock

This is normally the cable to use to connect the Digi to an X.21 leased line. Use this cable when the Digi is the clock *source* or configured as "internal clock".

DB 25 - Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
RxDA	2	2	TxDA
RxDB	3	9	TxDB
TxDA	4	4	RxDA
TxDB	5	11	RxDB
INDB	6	10	CTLB
GND	7	8	GND
CTLB	8	12	INDB
CLKB	15	13	CLKB
CLKA	17	6	CLKA
INDA	20	3	CTLA
CTLA	22	5	INDA

N.B. Frame Ground is optional.

X.21 25-Pin to 15-Pin Crossover Cable – External Clock

This is normally the cable to use to connect the Digi to an X.21 leased line. Use this cable when the Digi is the clock ***sink*** or configured as "external clock".

DB 25 - Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
RxDA	2	2	TxDA
RxDB	3	9	TxDB
TxDA	4	4	RxDA
TxDB	5	11	RxDB
INDB	6	10	CTLB
GND	7	8	GND
CTLB	8	12	INDB
CLKB	15	13	CLKB
CLKA	17	6	CLKA
INDA	20	3	CTLA
CTLA	22	5	INDA

N.B. Frame Ground is optional.

Note:

When operating an X.21 (RS-422) link Synchronously it is necessary to fit termination resistors to each signal pair at the receiving end. The Digi already has in-built terminating resistors, but terminating resistors will need to be fitted between the TxDA & TxDB pins, CLKA & CLKB pins and CTLA & CTLB pins at the DTE.

Port Pin-Outs

RS-232

			DB 25	RJ45
				
Description	**RS232 signal**	Direction[1]	Pin #	Pin #
Transmit Data	TxD	**in**	2	6
Receive Data	RxD	**out**	3	3
Ready To Send	RTS	**in**	4	1
Clear To Send	CTS	**out**	5	8
Data Set Ready	DSR	**out**	6	4
Ground	GND	**n/a**	7	5
Data Carrier Detect	DCD	**out**	8	7
Transmitter Clock	TxC	**out**	15	n/a
Receiver Clock	RxC	**out**	17	n/a
Data Terminal Ready	DTR	**in**	20	2
Ring Indicate	RI	**out**	22	n/a
External Transmitter Clock	ETC	**in**	24	n/a

1. With respect to Digi units

X.21 (RS-422)

Note:

In order for the IR2420 to operate in X.21 mode, an X.21 daughter card must be fitted, with the jumpers set correctly. See "Configuring X.21 on Older Models" on page 522.

			DB 25
			
Description	**X.21 signal**	Direction[1]	Pin #
Receive Data (A)	RxDA	**out**	2
Receive Data (B)	RxDB	**out**	3
Transmit Data (A)	TxDA	**in**	4
Transmit Data (B)	TxDB	**in**	5
Indication (B)	INDB	**out**	6
Ground	GND	**n/a**	7
Control (B)	CTLB	**in**	8
Clock (B)	CLKB	**in or out**[2]	15
Clock (A)	CLKA	**in or out**[2]	17
Indication (A)	INDA	**out**	20
Control (A)	CTLA	**in**	22

1. With respect to Digi units

2. Direction depends on whether the Digi unit is clock sink or clock source.

X.21 25-Pin to 15-Pin Straight Through Cable – Internal Clock

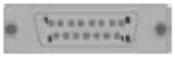
This is normally the cable to use to connect an X.21 terminal (e.g. an ATM) to the Digi. Use this cable when the Digi is the clock *source* or configured as "internal clock".

DB 25- Digi Side		DB 25	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
RxDA	2	4	RxDA
RxDB	3	11	RxDB
TxDA	4	2	TxDA
TxDB	5	9	TxDB
INDB	6	12	INDB
GND	7	8	GND
CTLB	8	10	CTLB
CLKB	15	13	CLKB
CLKA	17	6	CLKA
INDA	20	5	INDA
CTLA	22	3	CTLA

N.B. Frame Ground is optional.

X.21 25-Pin to 15-Pin Straight Through Cable – External Clock

This is normally the cable to use to connect an X.21 terminal (e.g. an ATM) to the Digi. Use this cable when the Digi is the clock ***sink*** or configured as "external clock".

DB 25- Digi Side		DB 25	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
RxDA	2	4	RxDA
RxDB	3	11	RxDB
TxDA	4	2	TxDA
TxDB	5	9	TxDB
INDB	6	12	INDB
GND	7	8	GND
CTLB	8	10	CTLB
CLKB	15	13	CLKB
CLKA	17	6	CLKA
INDA	20	5	INDA
CTLA	22	3	CTLA

N.B. Frame Ground is optional.

Note:

When operating an X.21 (RS-422) link Synchronously it is necessary to fit termination resistors to each signal pair at the receiving end. The Digi already has in-built terminating resistors, but terminating resistors will need to be fitted between the RxDA & RxDB pins, CLKA & CLKB pins and INDA & INDB pins at the DTE.

X.21 25-Pin to 15-Pin Crossover Cable – Internal Clock

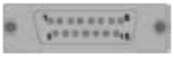
This is normally the cable to use to connect the Digi to an X.21 leased line. Use this cable when the Digi is the clock ***source*** or configured as "internal clock".

DB 25- Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
RxDA	2	2	TxDA
RxDB	3	9	TxDB
TxDA	4	4	RxDA
TxDB	5	11	RxDB
INDB	6	10	CTLB
GND	7	8	GND
CTLB	8	12	INDB
CLKB	15	13	CLKB
CLKA	17	6	CLKA
INDA	20	3	CTLA
CTLA	22	5	INDA

N.B. Frame Ground is optional.

X.21 25-Pin to 15-Pin Crossover Cable – External Clock

This is normally the cable to use to connect the Digi to an X.21 leased line. Use this cable when the Digi is the clock ***sink*** or configured as "external clock".

DB 25- Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
RxDA	2	2	TxDA
RxDB	3	9	TxDB
TxDA	4	4	RxDA
TxDB	5	11	RxDB
INDB	6	10	CTLB
GND	7	8	GND
CTLB	8	12	INDB
CLKB	15	13	CLKB
CLKA	17	6	CLKA
INDA	20	3	CTLA
CTLA	22	5	INDA

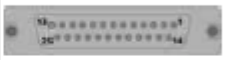
N.B. Frame Ground is optional.

Note:

When operating an X.21 (RS-422) link Synchronously it is necessary to fit termination resistors to each signal pair at the receiving end. The Digi already has in-built terminating resistors, but terminating resistors will need to be fitted between the TxDA & TxDB pins, CLKA & CLKB pins and CTLA & CTLB pins at the DTE.

Port Pin-Outs

RS-232

			DB 25	DB 9
				
Description	**RS232 signal**	Direction[1]	Pin #	Pin #
Transmit Data	TxD	**in**	2	3
Receive Data	RxD	**out**	3	2
Ready To Send	RTS	**in**	4	7
Clear To Send	CTS	**out**	5	8
Data Set Ready	DSR	**out**	6	6
Ground	GND	**n/a**	7	5
Data Carrier Detect	DCD	**out**	8	1
Transmitter Clock	TxC	**out**	15	n/a
Receiver Clock	RxC	**out**	17	n/a
Data Terminal Ready	DTR	**in**	20	4
Ring Indicate	RI	**out**	22	9
External Transmitter Clock	ETC	**in**	24	n/a

1. With respect to Digi units

X.21 (RS-422)

			DB 25	DB 9
				
Description	**X.21 signal**	Direction[1]	Pin #	Pin #
Transmit Data (A)	TxDA	**in**	2	1
Receive Data (A)	RxDA	**out**	3	2
Control (A)	CTLA	**in**	4	3
Indication (A)	INDA	**out**	5	4
Ground	GND	**n/a**	7	5
Clock (B)	CLKB	**in or out**[2]	9	n/a
Indication (B)	INDB	**out**	13	9
Transmit Data (B)	TxDB	**in**	14	6
Receive Data (B)	RxDB	**out**	16	7
Clock (A)	CLKA	**in or out**[2]	17	n/a
Control (B)	CTLB	**in**	19	8

1. With respect to Digi units
2. Direction depends on whether the Digi unit is clock sink or clock source.

X.21 25-Pin to 15-Pin Straight Through Cable – Internal Clock

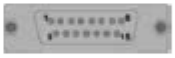
This is normally the cable to use to connect an X.21 terminal (e.g. an ATM) to the Digi. Use this cable when the Digi is the clock *source* or configured as "internal clock".

DB 25- Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
TxDA	2	2	TxDA
RxDA	3	4	RxDA
CTLA	4	3	CTLA
INDA	5	5	INDA
GND	7	8	GND
CLKB	9	13	CLKB
INDB	13	12	INDB
TxDB	14	9	TxDB
RxDB	16	11	RxDB
CLKA	17	6	CLKA
CTLB	19	10	CTLB

N.B. Frame Ground is optional.

X.21 25-Pin to 15-Pin Straight Through Cable – External Clock

This is normally the cable to use to connect an X.21 terminal (e.g. an ATM) to the Digi. Use this cable when the Digi is the clock ***sink*** or configured as "external clock".

DB 25- Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
TxDA	2	2	TxDA
RxDA	3	4	RxDA
CTLA	4	3	CTLA
INDA	5	5	INDA
GND	7	8	GND
CLKB	9	13	CLKB
INDB	13	12	INDB
TxDB	14	9	TxDB
RxDB	16	11	RxDB
CLKA	17	6	CLKA
CTLB	19	10	CTLB

N.B. Frame Ground is optional.

Note:

When operating an X.21 (RS-422) link Synchronously it is necessary to fit termination resistors to each signal pair at the receiving end. The Digi already has in-built terminating resistors, but terminating resistors will need to be fitted between the RxDA & RxDB pins, CLKA & CLKB pins and INDA & INDB pins at the DTE.

X.21 25-Pin to 15-Pin Crossover Cable – Internal Clock

This is normally the cable to use to connect the Digi to an X.21 leased line. Use this cable when the Digi is the clock *source* or configured as "internal clock".

DB 25- Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
TxDA	2	4	RxDA
RxDA	3	2	TxDA
CTLA	4	5	INDA
INDA	5	3	CTLA
GND	7	8	GND
CLKB	9	13	CLKB
INDB	13	10	CTLB
TxDB	14	11	RxDB
RxDB	16	9	TxDB
CLKA	17	6	CLKA
CTLB	19	12	INDB

N.B. Frame Ground is optional.

X.21 25-Pin to 15-Pin Crossover Cable – External Clock

This is normally the cable to use to connect the Digi to an X.21 leased line. Use this cable when the Digi is the clock ***sink*** or configured as "external clock".

DB 25- Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
TxDA	2	4	RxDA
RxDA	3	2	TxDA
CTLA	4	5	INDA
INDA	5	3	CTLA
GND	7	8	GND
CLKB	9	13	CLKB
INDB	13	10	CTLB
TxDB	14	11	RxDB
RxDB	16	9	TxDB
CLKA	17	6	CLKA
CTLB	19	12	INDB

N.B. Frame Ground is optional.

Note:

When operating an X.21 (RS-422) link Synchronously it is necessary to fit termination resistors to each signal pair at the receiving end. The Digi already has in-built terminating resistors, but terminating resistors will need to be fitted between the TxDA & TxDB pins, CLKA & CLKB pins and CTLA & CTLB pins at the DTE.

Port Pin-Outs

RS-232

			DB 25
			
Description	**RS232 signal**	Direction[1]	Pin #
Transmit Data	TxD	**in**	2
Receive Data	RxD	**out**	3
Ready To Send	RTS	**in**	4
Clear To Send	CTS	**out**	5
Data Set Ready	DSR	**out**	6
Ground	GND	**n/a**	7
Data Carrier Detect	DCD	**out**	8
Transmitter Clock	TxC	**out**	15
Receiver Clock	RxC	**out**	17
Data Terminal Ready	DTR	**in**	20
Ring Indicate	RI	**out**	22
External Transmitter Clock	ETC	**in**	24

1. With respect to Digi units

X.21 (RS-422)

			DB 25
			
Description	**X.21 signal**	Direction[1]	Pin #
Transmit Data (A)	TxDA	**in**	2
Receive Data (A)	RxDA	**out**	3
Control (A)	CTLA	**in**	4
Indication (A)	INDA	**out**	5
Ground	GND	**n/a**	7
Clock In (A)	CLKIA	**out**	9
Clock Out (B)	CLKOB	**in**	11
Indication (B)	INDB	**out**	13
Transmit Data (B)	TxDB	**in**	14
Receive Data (B)	RxDB	**out**	16
Clock In (B)	CLKIB	**out**	17
Control (B)	CTLB	**in**	19
Clock Out (A)	CLKOA	**in**	24

1. With respect to Digi units

X.21 25-Pin to 15-Pin Straight Through Cable – Internal Clock

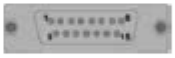
This is normally the cable to use to connect an X.21 terminal (e.g. an ATM) to the Digi. Use this cable when the Digi is the clock *source* or configured as "internal clock".

DB 25- Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
TxDA	2	2	TxDA
RxDA	3	4	RxDA
CTLA	4	3	CTLA
INDA	5	5	INDA
GND	7	8	GND
CLKA	9	6	CLKA
INDB	13	12	INDB
TxDB	14	9	TxDB
RxDB	16	11	RxDB
CLKB	17	13	CLKB
CTLB	19	10	CTLB

N.B. Frame Ground is optional.

X.21 25-Pin to 15-Pin Straight Through Cable – External Clock

This is normally the cable to use to connect an X.21 terminal (e.g. an ATM) to the Digi. Use this cable when the Digi is the clock *sink* or configured as "external clock".

DB 25 - Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
TxDA	2	2	TxDA
RxDA	3	4	RxDA
CTLA	4	3	CTLA
INDA	5	5	INDA
GND	7	8	GND
CLKB	11	13	CLKB
INDB	13	12	INDB
TxDB	14	9	TxDB
RxDB	16	11	RxDB
CTLB	19	10	CTLB
CLKA	24	6	CLKA

N.B. Frame Ground is optional.

Note:

When operating an X.21 (RS-422) link Synchronously it is necessary to fit termination resistors to each signal pair at the receiving end. The Digi already has in-built terminating resistors, but terminating resistors will need to be fitted between the TxDA & TxDB pins, CLKA & CLKB pins and CTLA & CTLB pins at the DTE.

X.21 25-Pin to 15-Pin Crossover Cable – Internal Clock

This is normally the cable to use to connect the Digi to an X.21 leased line. Use this cable when the Digi is the clock *source* or configured as "internal clock".

DB 25 - Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
TxDA	2	4	RxDA
RxDA	3	2	TxDA
CTLA	4	5	INDA
INDA	5	3	CTLA
GND	7	8	GND
CLKA	9	6	CLKA
INDB	13	10	CTLB
TxDB	14	11	RxDB
RxDB	16	9	TxDB
CLKB	17	13	CLKB
CTLB	19	12	INDB

N.B. Frame Ground is optional.

X.21 25-Pin to 15-Pin Crossover Cable – External Clock

This is normally the cable to use to connect the Digi to an X.21 leased line. Use this cable when the Digi is the clock ***sink*** or configured as "external clock".

DB 25 - Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
TxDA	2	4	RxDA
RxDA	3	2	TxDA
CTLA	4	5	INDA
INDA	5	3	CTLA
GND	7	8	GND
CLKB	11	13	CLKB
INDB	13	10	CTLB
TxDB	14	11	RxDB
RxDB	16	9	TxDB
CTLB	19	12	INDB
CLKA	24	6	CLKA

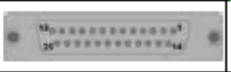
N.B. Frame Ground is optional

Note:

When operating an X.21 (RS-422) link Synchronously it is necessary to fit termination resistors to each signal pair at the receiving end. The Digi already has in-built terminating resistors, but terminating resistors will need to be fitted between the TxDA & TxDB pins, CLKA & CLKB pins and CTLA & CTLB pins at the DTE.

Port Pin-Outs

RS-232

			DB 25	RJ45
				
Description	**RS232 signal**	Direction[1]	Pin #	Pin #
Transmit Data	TxD	**in**	2	6
Receive Data	RxD	**out**	3	3
Ready To Send	RTS	**in**	4	1
Clear To Send	CTS	**out**	5	8
Data Set Ready	DSR	**out**	6	4
Ground	GND	**n/a**	7	5
Data Carrier Detect	DCD	**out**	8	7
Transmitter Clock	TxC	**out**	15	n/a
Receiver Clock	RxC	**out**	17	n/a
Data Terminal Ready	DTR	**in**	20	2
Ring Indicate	RI	**out**	22	n/a
External Transmitter Clock	ETC	**in**	24	n/a

1. With respect to Digi units

X.21 (RS-422)

Note:

In order for the MW3410, MW3520 or VC5100 to operate in X.21 mode, an X.21 daughter card must be fitted.

			DB 25
			
Description	**X.21 signal**	Direction[1]	Pin #
Receive Data (A)	RxDA	**out**	2
Receive Data (B)	RxDB	**out**	3
Transmit Data (A)	TxDA	**in**	4
Transmit Data (B)	TxDB	**in**	5
Indication (B)	INDB	**out**	6
Ground	GND	**n/a**	7
Control (B)	CTLB	**in**	8
Clock (A)	CLKA	**in or out**[2]	15
Clock (B)	CLKB	**in or out**[2]	17
Indication (A)	INDA	**out**	20
Control (A)	CTLA	**in**	22

1. With respect to Digi units
2. Direction depends on whether Digi unit is clock sink or clock source.

X.21 25-Pin to 15-Pin Straight Through Cable – Internal Clock

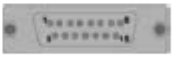
This is normally the cable to use to connect an X.21 terminal (e.g. an ATM) to the Digi. Use this cable when the Digi is the clock *source* or configured as "internal clock".

DB 25 - Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
RxDA	2	4	RxDA
RxDB	3	11	RxDB
TxDA	4	2	TxDA
TxDB	5	9	TxDB
INDB	6	12	INDB
GND	7	8	GND
CTLB	8	10	CTLB
CLKA	15	6	CLKA
CLKB	17	13	CLKB
INDA	20	5	INDA
CTLA	22	3	CTLA

N.B. Frame Ground is optional.

X.21 25-Pin to 15-Pin Straight Through Cable – External Clock

This is normally the cable to use to connect an X.21 terminal (e.g. an ATM) to the Digi. Use this cable when the Digi is the clock *sink* or configured as "external clock".

DB 25 - Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
RxDA	2	4	RxDA
RxDB	3	11	RxDB
TxDA	4	2	TxDA
TxDB	5	9	TxDB
INDB	6	12	INDB
GND	7	8	GND
CTLB	8	10	CTLB
CLKA	15	13	CLKA
CLKB	17	6	CLKB
INDA	20	5	INDA
CTLA	22	3	CTLA

N.B. Frame Ground is optional.

Note:

When operating an X.21 (RS-422) link Synchronously it is necessary to fit termination resistors to each signal pair at the receiving end. The Digi already has in-built terminating resistors, but terminating resistors will need to be fitted between the TxDA & TxDB pins, CLKA & CLKB pins and CTLA & CTLB pins at the DTE.

X.21 25-Pin to 15-Pin Crossover Cable – Internal Clock

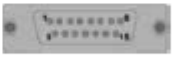
This is normally the cable to use to connect the Digi to an X.21 leased line. Use this cable when the Digi is the clock ***source*** or configured as "internal clock".

DB 25 - Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
RxDA	2	2	TxDA
RxDB	3	9	TxDB
TxDA	4	4	RxDA
TxDB	5	11	RxDB
INDB	6	10	CTLB
GND	7	8	GND
CTLB	8	12	INDB
CLKA	15	13	CLKA
CLKB	17	6	CLKB
INDA	20	3	CTLA
CTLA	22	5	INDA

N.B. Frame Ground is optional.

X.21 25-Pin to 15-Pin Crossover Cable – External Clock

This is normally the cable to use to connect the Digi to an X.21 leased line. Use this cable when the Digi is the clock ***sink*** or configured as "external clock".

DB 25 - Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
RxDA	2	2	TxDA
RxDB	3	9	TxDB
TxDA	4	4	RxDA
TxDB	5	11	RxDB
INDB	6	10	CTLB
GND	7	8	GND
CTLB	8	12	INDB
CLKA	15	13	CLKA
CLKB	17	6	CLKB
INDA	20	3	CTLA
CTLA	22	5	INDA

N.B. Frame Ground is optional.

Note:

When operating an X.21 (RS-422) link Synchronously it is necessary to fit termination resistors to each signal pair at the receiving end. The Digi already has in-built terminating resistors, but terminating resistors will need to be fitted between the TxDA & TxDB pins, CLKA & CLKB pins and CTLA & CTLB pins at the DTE.

ER4420, ER4420d, ER4420i, ER4420p, HR4420, HR4420d, HR4420i, HR4420p & IR4420

Port Pin-Outs

RS-232

			DB 25
			
Description	**RS232 signal**	Direction[1]	Pin #
Transmit Data	TxD	**in**	2
Receive Data	RxD	**out**	3
Ready To Send	RTS	**in**	4
Clear To Send	CTS	**out**	5
Data Set Ready	DSR	**out**	6
Ground	GND	**n/a**	7
Data Carrier Detect	DCD	**out**	8
Transmitter Clock	TxC	**out**	15
Receiver Clock	RxC	**out**	17
Data Terminal Ready	DTR	**in**	20
Ring Indicate	RI	**out**	22
External Transmitter Clock	ETC	**in**	24

1. With respect to Digi units

X.21 (RS-422)

			DB 25
			
Description	**X.21 signal**	Direction[1]	Pin #
Transmit Data (A)	TxDA	**in**	2
Receive Data (A)	RxDA	**out**	3
Control (A)	CTLA	**in**	4
Indication (A)	INDA	**out**	5
Ground	GND	**n/a**	7
Clock In (B)	CLKIB	**out**	9
Clock Out (B)	CLKOB	**in**	11
Indication (B)	INDB	**out**	13
Transmit Data (B)	TxDB	**in**	14
Receive Data (B)	RxDB	**out**	16
Clock In (A)	CLKIA	**out**	17
Control (B)	CTLB	**in**	19
Clock Out (A)	CLKOA	**in**	24

1. With respect to Digi units

X.21 25-Pin to 15-Pin Straight Through Cable – Internal Clock

This is normally the cable to use to connect an X.21 terminal (e.g. an ATM) to the Digi. Use this cable when the Digi is the clock *source* or configured as "internal clock".

DB 25 - Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
TxDA	2	2	TxDA
RxDA	3	4	RxDA
CTLA	4	3	CTLA
INDA	5	5	INDA
GND	7	8	GND
CLKB	9	13	CLKB
INDB	13	12	INDB
TxDB	14	9	TxDB
RxDB	16	11	RxDB
CLKA	17	6	CLKA
CTLB	19	10	CTLB

N.B. Frame Ground is optional.

X.21 25-Pin to 15-Pin Straight Through Cable – External Clock

This is normally the cable to use to connect an X.21 terminal (e.g. an ATM) to the Digi. Use this cable when the Digi is the clock ***sink*** or configured as "external clock".

DB 25 - Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
TxDA	2	2	TxDA
RxDA	3	4	RxDA
CTLA	4	3	CTLA
INDA	5	5	INDA
GND	7	8	GND
CLKB	11	13	CLKB
INDB	13	12	INDB
TxDB	14	9	TxDB
RxDB	16	11	RxDB
CTLB	19	10	CTLB
CLKA	24	6	CLKA

N.B. Frame Ground is optional.

Note:

When operating an X.21 (RS-422) link Synchronously it is necessary to fit termination resistors to each signal pair at the receiving end. The Digi already has in-built terminating resistors, but terminating resistors will need to be fitted between the TxDA & TxDB pins, CLKA & CLKB pins and CTLA & CTLB pins at the DTE.

X.21 25-Pin to 15-Pin Crossover Cable – Internal Clock

This is normally the cable to use to connect the Digi to an X.21 leased line. Use this cable when the Digi is the clock *source* or configured as "internal clock".

DB 25 - Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
TxDA	2	4	RxDA
RxDA	3	2	TxDA
CTLA	4	5	INDA
INDA	5	3	CTLA
GND	7	8	GND
CLKB	9	13	CLKB
INDB	13	10	CTLB
TxDB	14	11	RxDB
RxDB	16	9	TxDB
CLKA	17	6	CLKA
CTLB	19	12	INDB

N.B. Frame Ground is optional.

X.21 25-Pin to 15-Pin Crossover Cable – External Clock

This is normally the cable to use to connect the Digi to an X.21 leased line. Use this cable when the Digi is the clock ***sink*** or configured as "external clock".

DB 25 - Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
TxDA	2	4	RxDA
RxDA	3	2	TxDA
CTLA	4	5	INDA
INDA	5	3	CTLA
GND	7	8	GND
CLKB	11	13	CLKB
INDB	13	10	CTLB
TxDB	14	11	RxDB
RxDB	16	9	TxDB
CTLB	19	12	INDB
CLKA	24	6	CLKA

N.B. Frame Ground is optional.

Note:

When operating an X.21 (RS-422) link Synchronously it is necessary to fit termination resistors to each signal pair at the receiving end. The Digi already has in-built terminating resistors, but terminating resistors will need to be fitted between the TxDA & TxDB pins, CLKA & CLKB pins and CTLA & CTLB pins at the DTE.

Port Pin-Outs

RS-232

			DB 25
			
Description	**RS232 signal**	Direction[1]	Pin #
Transmit Data	TxD	**in**	2
Receive Data	RxD	**out**	3
Ready To Send	RTS	**in**	4
Clear To Send	CTS	**out**	5
Data Set Ready	DSR	**out**	6
Ground	GND	**n/a**	7
Data Carrier Detect	DCD	**out**	8
Transmitter Clock	TxC	**out**	15
Receiver Clock	RxC	**out**	17
Data Terminal Ready	DTR	**in**	20
Ring Indicate	RI	**out**	22
External Transmitter Clock	ETC	**in**	24

1. With respect to Digi units

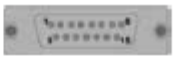
X.21 (RS-422)

			DB 25
			
Description	**X.21 signal**	Direction[1]	Pin #
Transmit Data (A)	TxDA	**in**	2
Receive Data (A)	RxDA	**out**	3
Control (A)	CTLA	**in**	4
Indication (A)	INDA	**out**	5
Ground	GND	**n/a**	7
Clock In (B)	CLKIB	**out**	9
Clock Out (B)	CLKOB	**in**	11
Indication (B)	INDB	**out**	13
Transmit Data (B)	TxDB	**in**	14
Receive Data (B)	RxDB	**out**	16
Clock In (A)	CLKIA	**out**	17
Control (B)	CTLB	**in**	19
Clock Out (A)	CLKOA	**in**	24

1. With respect to Digi units

X.21 25-Pin to 15-Pin Straight Through Cable – Internal Clock

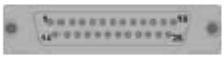
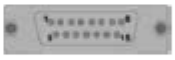
This is normally the cable to use to connect an X.21 terminal (e.g. an ATM) to the Digi. Use this cable when the Digi is the clock ***source*** or configured as "internal clock".

DB 25 - Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
TxDA	2	2	TxDA
RxDA	3	4	RxDA
CTLA	4	3	CTLA
INDA	5	5	INDA
GND	7	8	GND
CLKB	9	13	CLKB
INDB	13	12	INDB
TxDB	14	9	TxDB
RxDB	16	11	RxDB
CLKA	17	6	CLKA
CTLB	19	10	CTLB

N.B. Frame Ground is optional.

X.21 25-Pin to 15-Pin Straight Through Cable – External Clock

This is normally the cable to use to connect an X.21 terminal (e.g. an ATM) to the Digi. Use this cable when the Digi is the clock ***sink*** or configured as "external clock".

DB 25 - Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
TxDA	2	2	TxDA
RxDA	3	4	RxDA
CTLA	4	3	CTLA
INDA	5	5	INDA
GND	7	8	GND
CLKB	11	13	CLKB
INDB	13	12	INDB
TxDB	14	9	TxDB
RxDB	16	11	RxDB
CTLB	19	10	CTLB
CLKA	24	6	CLKA

N.B. Frame Ground is optional.

Note:

When operating an X.21 (RS-422) link Synchronously it is necessary to fit termination resistors to each signal pair at the receiving end. The Digi already has in-built terminating resistors, but terminating resistors will need to be fitted between the TxDA & TxDB pins, CLKA & CLKB pins and CTLA & CTLB pins at the DTE.

X.21 25-Pin to 15-Pin Crossover Cable – Internal Clock

This is normally the cable to use to connect the Digi to an X.21 leased line. Use this cable when the Digi is the clock *source* or configured as "internal clock".

DB 25 - Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
TxDA	2	4	RxDA
RxDA	3	2	TxDA
CTLA	4	5	INDA
INDA	5	3	CTLA
GND	7	8	GND
CLKB	9	13	CLKB
INDB	13	10	CTLB
TxDB	14	11	RxDB
RxDB	16	9	TxDB
CLKA	17	6	CLKA
CTLB	19	12	INDB

N.B. Frame Ground is optional.

X.21 25-Pin to 15-Pin Crossover Cable – External Clock

This is normally the cable to use to connect the Digi to an X.21 leased line. Use this cable when the Digi is the clock ***sink*** or configured as "external clock".

DB 25 - Digi Side		DB 15	
			
Signal	**Pin # (DCE)**	**Pin # (DTE)**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
TxDA	2	4	RxDA
RxDA	3	2	TxDA
CTLA	4	5	INDA
INDA	5	3	CTLA
GND	7	8	GND
CLKB	11	13	CLKB
INDB	13	10	CTLB
TxDB	14	11	RxDB
RxDB	16	9	TxDB
CTLB	19	12	INDB
CLKA	24	6	CLKA

N.B. Frame Ground is optional.

Note:

When operating an X.21 (RS-422) link Synchronously it is necessary to fit termination resistors to each signal pair at the receiving end. The Digi already has in-built terminating resistors, but terminating resistors will need to be fitted between the TxDA & TxDB pins, CLKA & CLKB pins and CTLA & CTLB pins at the DTE.

RS-232 (V.24) Serial Cable Wiring

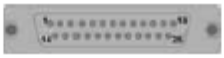
The tables below detail the wiring required for the various types of serial cable that you may need.

Note:

Some products are able to operate both Synchronously and Asynchronously. When these products are operating Asynchronously, it is strongly recommended that the Clock pins (TxC, RxC and ETC) are left disconnected.

25-Pin to 25-Pin Straight Through Cable

This is normally the cable to use to connect a V.24 synchronous terminal to a Digi router.

DB 25 - Digi Side		DB 25	
			
Signal	**Pin #**	**Pin #**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
TxD	2	2	TxD
RxD	3	3	RxD
RTS	4	4	RTS
CTS	5	5	CTS
DSR	6	6	DSR
GND	7	7	GND
DCD	8	8	DCD
RxC	17	17	RxC
DTR	20	20	DTR
ETC	24	24	ETC

N.B. Frame Ground is optional.

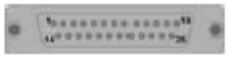
25-Pin to 9-Pin Straight Through Cable

This is normally the cable to use to connect a V.24 asynchronous terminal (such as a PC) to a Digi router.

DB 25 - Digi Side		DB 9	
			
Signal		**Pin #**	**Signal**
TxD	2	3	TxD
RxD	3	2	RxD
RTS	4	7	RTS
CTS	5	8	CTS
DSR	6	6	DSR
GND	7	5	GND
DCD	8	1	DCD
DTR	20	4	DTR
RING	22	9	RING

RJ45 to 25-Pin Straight Through Cable

This is normally the cable to use to connect a V.24 synchronous terminal to a Digi router.

RJ45 - Digi Side		DB 25	
			
Signal	**Pin #**	**Pin#**	**Signal**
RTS	1	4	RTS
DTR	2	20	DTR
RxD	3	3	RxD
GND	5	7	GND
TxD	6	2	TxD
DCD	7	8	DCD
CTS	8	5	CTS

RJ45 to 9-Pin Straight Through Cable

This is normally the cable to use to connect a V.24 asynchronous terminal (such as a PC) to a Digi router.

RJ45 - Digi Side		DB 9	
			
Signal	**Pin #**	**Pin#**	**Signal**
RTS	1	7	RTS
DTR	2	4	DTR
RxD	3	2	RxD
GND	5	5	GND
TxD	6	3	TxD
DCD	7	1	DCD
CTS	8	8	CTS

25-Pin to 25-Pin Crossover Cable

This is normally the cable to use to connect the router to a V.24 leased line.

DB 25 - Digi Side		DB 25	
			
Signal	**Pin #**	**Pin #**	**Signal**
Frame Ground (Case)	Shield	Shield	Frame Ground (Case)
TxD	2	3	RxD
RxD	3	2	TxD
RTS	4	5	CTS
CTS	5	4	RTS
GND	7	7	GND
DCD	8	20	DTR
RxC	17	24	ETC
DTR	20	8	DCD
ETC	24	17	RxC

N.B. Frame Ground is optional.

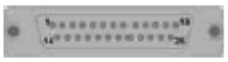
25-Pin to 9-Pin Crossover Cable

This cable would normally be used to connect the router to an external asynchronous modem.

DB 25 - Digi Side		DB 9	
			
Signal	**Pin #**	**Pin #**	**Signal**
TxD	2	2	RxD
RxD	3	3	TxD
RTS	4	8	CTS
CTS	5	7	RTS
GND	7	5	GND
DCD	8	4	DTR
DTR	20	1	DCD

RJ45 to 25-Pin Crosssover Cable

This is normally the cable to use to connect the router to a V.24 leased line.

RJ45 - Digi Side		DB 25	
			
Signal	**Pin #**	**Pin#**	**Signal**
RTS	1	5	CTS
DTR	2	8	DCD
RxD	3	2	TxD
GND	5	7	GND
TxD	6	3	RxD
DCD	7	20	DTR
CTS	8	4	RTS

RJ45 to 9-Pin Crossover Cable

This cable would normally be used to connect the router to an external asynchronous modem.

RJ45 - Digi Side		DB 9	
			
Signal	**Pin #**	**Pin#**	**Signal**
RTS	1	8	CTS
DTR	2	1	DCD
RxD	3	3	TxD
GND	5	5	GND
TxD	6	2	RxD
DCD	7	4	DTR
CTS	8	7	RTS

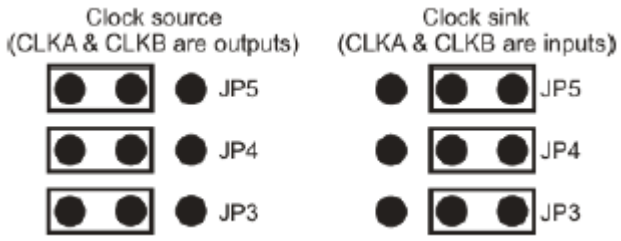
Configuring X.21 on Older Models

Some older Sarian legacy units require an X.21 daughter card to be fitted to enable X.21 operation. There are two versions of the X.21 daughter card. One version is compatible with GR2130, IR2140 and IR2420 routers, and one version is compatible with MW3520, MW3410 and VC5100 routers.

The X.21 daughter card compatible with GR2130, IR2140 and IR2420 routers has three internal jumpers that determine the clock mode. By default, these are set so that the unit acts as a clock sink. For correct X.21 operation the jumper settings must match the setting of the Clock source parameter configured on the Configuration - Network > Interfaces > Serial > Serial Port 0 > Sync Port 0 pages. To change this you will need to open the unit by removing the four rubber feet and fixing screws. Having done this, carefully remove the case lid and locate the X.21 adapter card (illustrated below):



The correct settings for clock source or clock sink operation for the X.21 daughter card compatible with GR2130, IR2140 and IR2420 routers are shown below:



Having set the links correctly, reassemble the case ensuring that the lid is correctly oriented.

EMAIL TEMPLATES

One of the principal features provided by the event log function is the ability to configure the unit to automatically generate and send an email alert message each time an event of up to a specified priority occurs. The format of the message is determined by the email template specified in the **Use email template file** parameter (normally EVENT.EML) in the ***Configuration - Alarms > Event Settings > Email Notifications*** web page.

If the standard EVENT.EML template supplied with the unit is not suitable, you may create your own template. An email template is simply a text file that defines the appearance and content of the email messages generated by the event logger.

Template Structure

An email template consists of a header section followed by a body section. One or more blank lines separate the two sections.

The Header Section

The header section MUST contain the following three fields:

TO:

This field is used to specify at least one recipient's email address. Multiple addresses may be included and must be separated by a space, comma or semicolon character. For example:

To: 123@456.com, 456@123.com; abc.def.com

FROM:

This field is normally used to supply the email address of the sending unit but alternatively you may enter a simple string. This may depend on the SMTP server as to what is accepted. For example:

FROM: WR44

Or

FROM: wr44@mycompany.com

SUBJECT:

This field should contain a string describing the subject of the email message. For example:

Subject: Automated message from router

Other Fields

In addition to the mandatory fields described above, the header section of an email may also contain one or more optional fields. Many such fields are defined in the relevant RFCs but there are some fields that the unit handles a little differently as described below. The unit will insert other fields as necessary if it is required to send attachments with the email

Reply To:

If the unit discovers that this field is not present in the email template, the unit will insert this field into the header. The string used for this field is that configured by the *smtp 0 reply_to* CLI command (or the use "**Reply To**" address parameter in the ***Configuration - Alarms > SMTP Account*** web page). This allows for different reply addresses, and allows a simple way of using the same (easily configurable) reply address for all emails.

Date:

If this field is present in the header, the unit will insert the current date and time into the header. The date and time are values local to the unit and do not contain any time zone information.

Body Section

The body section may include any text. This text is parsed for any function calls that may be present. Function calls must be enclosed between "<%" and "%>". These sequences are substituted by text resulting from the function call. The following functions may be used:

Function	Description
TimeSmtp();	Inserts the unit's date and time.
serial_number();	Inserts the unit's serial number
Smtpip();	Inserts the IP address of the unit as seen by the SMTP server during transmission
email_event()	Inserts a formatted description of the event that caused the email transmission.
Smtpid()	Inserts the unit ID for this device as configured by the "Router Identity" field in the Configuration - System > Device Identity web page, or the cmd 0 unitid CLI command.
pppip("instance");	Inserts the IP address for a specific PPP instance, where instance is the PPP instance number.

The following are examples of email templates.

```
1)
TO: 123@abc.co.nz
FROM: MyRouter
SUBJECT: Remote Configuration
                                        ← This blank line is required
Time: <%timeSmtp();%>
Serial Number: <%serial_number();%>
Req: CFG_RQ
IP Address: <%smtpip();%>
PPP 1 IP address: <%pppip("1");%>
```

```
2)
TO: fred@anyco.com, jane@anyco.co.uk
FROM: MyRouter
SUBJECT: automatic email
MIME-Version: 1.0
                                        ← This blank line is required
Unit: <%smtpid();%>
Event: <%email_event();%>
This event had sufficient priority to cause the transmission of this
email. Please check the attached logs and review.
```

CLI commands can also be executed and the output from up to 10 CLI commands will be added to the body of the email. The command to be executed needs to be entered in place of xxxxx below. To include the output from multiple commands, use the run_cmd() function multiple times.

```
<%run_cmd("xxxxx");%>
```

e.g.

```
<%run_cmd("ati5");%>
<%run_cmd("bufs");%>
<%run_cmd("msgs");%>
```

An example template adding CLI commands would be:

```
TO: fred@anyco.com, jane@anyco.co.uk
FROM: MyRouter
SUBJECT: automatic email
MIME-Version: 1.0

Unit: <%smtpid();%>
Event: <%email_event();%>
This event had sufficient priority to cause the transmission of this
email. Please check the attached logs and review.
<%run_cmd("ati5");%>
<%run_cmd("bufs");%>
<%run_cmd("msgs");%>
```

It is also possible to specify an extra parameter which indicates the required priority of the event before the command is executed. This allows events to be sent off without attachments, but if the event has an equal or higher priority than the value of this parameter, the attachments will be included. This ensures that the attachments are not included unnecessarily with non-critical events and using up all the data allowance on a wireless connection.

```
<%run_cmd("chkst","5");%>
```

An example template adding CLI commands with priority values would be:

```
TO: fred@anyco.com, jane@anyco.co.uk
FROM: MyRouter
SUBJECT: automatic email
MIME-Version: 1.0

Unit: <%smtpid();%>
Event: <%email_event();%>
This event had sufficient priority to cause the transmission of this
email. Please check the attached logs and review.
<%run_cmd("chkst","5");%>
```

In the example above, the command chkst will only be executed when an event with a priority equal to or higher than 5 is detected.

Certifications

FCC Part 68 Declarations (for Transport DR models only)

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the underside of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. If requested, this number must be provided to the telephone company.

Universal Service Order Codes

RJ11C

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instructions for details.

Telephone Company Compliance

If the Transport DR, causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service. If trouble is experienced with the Transport DR, for repair or warranty information, please contact Digi International at 877-912-3444. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

The REN is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is noted in the part of the product identifier that has the format US:AAAEQ##TXXXX. The digits represented by the ## are the REN without a decimal point (e.g., 03 is a REN of 0.3). For early products, the REN is shown separately on the label.

Home Security Advisory

If your home has specially wired alarm equipment connected to the telephone line, ensure the installation of this Transport DR does not disable your alarm equipment. If you have questions about what will disable alarm equipment, consult your telephone company or a qualified installer.

OEM Advisory

For OEM use, the mounting of the Transport DR in the final assembly must be made so that the Transport DR is isolated from exposure to any hazardous voltages within the assembly. Adequate separation and restraint of cables and cords must be provided. The circuitry from the Transport DR to the telephone line must be provided in wiring that carries no other circuitry (such as PC or PR leads) unless specifically allowed by the rules. PC board traces carrying tip and ring leads shall have sufficient spacing to avoid surge breakdown.

Electrical Safety Advisory

Digi International suggests that customers use a surge arrestor. Telephone companies report that electrical surges, typically lightning transients, are very destructive to customer terminal equipment connected to AC power sources. This has been identified as a major nationwide problem.

GLOSSARY

0 - 9

3DES	Triple Data Encryption Standard

A

ACCM	Asynchronous Communication Channel Multiplexer
ACFC	Address Control Field Compression
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
AFE	Analogue Front End
AH	Authentication Header
AIS	Alarm Indication Signal
AODI	Always On Dynamic ISDN
APACS	Association of Payment Clearing Services, the UK payments association
APN	Access Point Name
ATM	Asynchronous Transfer Mode or Automatic Teller Machine
ARFCN	Absolute Radio Frequency Channel Number

B

BACP	Bandwidth Allocation and Control Protocol
BAP	Bandwidth Allocation Protocol
BCC	Base station Colour Code
BCCH	Broadcast Control Channel
BGP	Border Gateway Protocol

C

CA	Certificate Authority
CHAP	Challenge Handshake Authentication Protocol
CLI	Calling Line Identification or Command Line Interface
CRC	Cyclic Redundancy Code
CTS	Clear To Send
CUD	Call User Data
CUG	Call User Group

D

DCE	Data Communication Equipment
DER	Distinguished Encoding Rules
DES	Data Encryption Standard

DHCP	Dynamic Host Configuration Protocol
DLSw	Data-Link Switching
DNS	Domain Name Server
DPD	Dead Peer Detection
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber Line
DTE	Data Terminal Equipment
DUN	Dial-Up Networking

E

EDGE	Enhanced Data GSM Environment
ESP	Encapsulating Security Payload protocol

F

FCS	Frame Check Sequence
FEC	Forward Error Correction
FIFO	First In First Out
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol

G

GPRS	General Packet Radio System
GPS	Global Positioning System
GRE	Generic Routing Encapsulation
GSM	Global System for Mobile Communications

H

HDLC	High-Level Data Link Control
HEC	Header Error Control
HMAC	Hash Message Authentication Code
HSDPA	High Speed Downlink Packet Access
HSUPA	High Speed Uplink Packet Access

I

ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IKE	Internet Key Exchange
IMEI	International Mobile Equipment Identification

IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
IPSec	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network

L

L2TP	Layer 2 Tunnelling Protocol
LAC	Location Area Code
LAI	Location Area Identity
LAN	Local Area Network
LAPB	Link Access Procedure Balanced
LAPD	Link Access Protocol D-channel
LCN	Logical Channel Number
LCP	Link Control Protocol
LRC	Longitudinal Redundancy Check
LSA	Link State Advertisement

M

MAC	Media Access Control
MCC	Mobile Country Code
MD5	Message-Digest algorithm 5
MIB	Management Information Base
MIME	Multipurpose Internet Mail Extensions
MLPPP	Multi-Link Point-to-Point Protocol
MNC	Mobile Network Code
MPPE	Microsoft Point to Point Encryption
MRU	Maximum Receive Unit
MSN	Multiple Subscriber Number
MSS	Maximum Segment Size
MTU	Maximum Transmit Unit

N

NAPT	Network Address and Port Translation
NAS	Network Access Server
NAT	Network Address Translation
NCC	Network Colour Code

NOM	Network Operation Mode
NUA	Network User Address
NUI	Network User Identifier

O

OAM	Operation, Administration and Maintenance
OOS	Out Of Service
OPNS	Online PUK Negotiation Service
OSPF	Open Shortest Path First

P

PANS	Polling Answering Service
PAD	Packet Assembler/Disassembler
PAP	Password Authentication Protocol
PAT	Priority Access Threshold
PBCCH	Packet Broadcast Control Channel
PEM	Privacy Enhanced MIME
PFC	Protocol Field Compression
PFS	Perfect Forwarding Security
PID	Protocol Identifier
PIN	Personal Identity Number
PLMN	Public Land Mobile Network
PPP	Point-to-Point Protocol
PPPoA	Point-to-Point Protocol over ATM
PPPoE	Point-to-Point Protocol over Ethernet
PSDN	Packet Switched Data Network
PSI	Packet System Information
PSTN	Public Switched Telephone Network
PUK	Power Up Key
PVC	Permanent Virtual Circuit

Q

QOS	Quality of Service

R

RAC	Routing Area Code
RACH	Random Access Channel
RADIUS	Remote Authentication Dial-In User Service
RAT	Radio Access Technology
RDI	Remote Defect Indication
RIP	Routing Information Protocol
RSSI	Received Signal Strength Indication
RTS	Request To Send

S

SA	Security Association
SABM	Set Asynchronous Balanced Mode
SABME	Set Asynchronous Balanced Mode Extended
SCEP	Simple Certificate Enrolment Protocol
SDLC	Synchronous Data Link Control
SHA-1	Secure Hash Algorithm 1
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNA	Systems Network Architecture
SNAIP	Systems Network Architecture over Internet Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SPF	Shortest Path First
SPI	Security Parameters Index
SSH	Secure Shell
SSL	Secure Socket Layer
SVC	Switched Virtual Circuit

T

TANS	TPAD Answering
TCH	Traffic Channel
TCP	Transmission Control Protocol
TEI	Terminal Endpoint Identifier
TOS	Type of Service
TPAD	Transaction Packet Assembler/Disassembler

U	
UBR	Unspecified Bit Rate
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
V	
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
W	
WAN	Wide Area Network
WCDMA	Wide-band Code-Division Multiple Access
WRED	Weighted Random Early Dropping
W-WAN	Wireless Wide Area Network
X	
XOT	X.25 Over TCP

ACKNOWLEDGEMENTS

Copyright Digi International Limited 1999-2011, all rights reserved.

In addition we would like to thank all those who have contributed to open software which has done so much to improve and expand knowledge of IP protocols and the Internet generally.

Notably software in this product contains portions of code from the OpenBSD project under the following copyrights:

Copyright (c) 2003, 2004 Henning Brauer <henning@openbsd.org>

Copyright (c) 2004 Esben Norby <norby@openbsd.org>

Copyright (c) 2001 Markus Friedl. All rights reserved.

Copyright (c) 2001 Daniel Hartmeier. All rights reserved.

Copyright (c) 2001 Theo de Raadt. All rights reserved.

Copyright (c) 2001 Tobias Weingartner

This product also includes cryptographic software written by

Eric Young (eay@cryptsoft.com) copyright (C) 1995-1997 Eric Young (eay@cryptsoft.com)

Web Interface

Copyright (c) Go Ahead Software Inc., 1995-1999. All Rights Reserved.

Zlib compression library

Copyright (C) 1995-1998 Jean-loup Gailly and Mark Adler

Digi TransPort 6000 Series Routers

Portions Copyright Centillium Communications, Inc. 2003

Sarian Systems / Digi TransPort 3000 and 5000 series routers

Portions Copyright 2000-2002 Intel Corporation All Rights Reserved

Sarian Systems / Digi TransPort 4000 series Routers

Portions copyright (c) 2001,2002,2003,2004 Cirrus Logic, Inc.

All 2000, 3000, 4000 and 5000 series units:

Portions Copyright © ARM Limited 1998, 1999. All rights reserved.

Portions of this code:

Copyright (c) 1998, 1999 Niels Provos.

(c) 1999 Angelos D. Keromytis. All rights reserved.

Copyright (c) 2000, 2001 Niklas Hallqvist. All rights reserved.

In addition we would like to thank Peter Verhas for his outstanding work on the ScriptBasic Interpreter, a SarOS Ported version together with libraries for many telemetry devices can be provided free with any suitable Sarian Systems / Digi TransPort product. Several files in this release of ScriptBasic are available under the GNU LPGL and full terms together with source and linkable libraries are available on request.